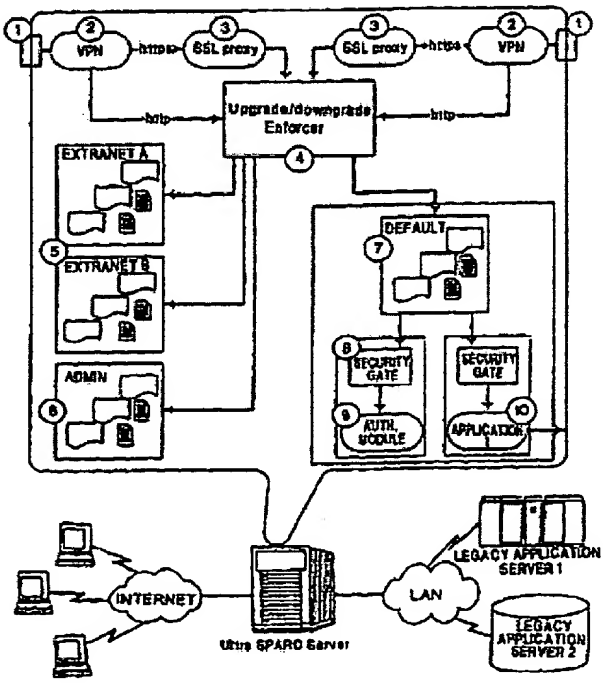
TRUSTED COMPARTMENTALIZED COMPUTER OPERATING SYSTEM

Publication number: JP2002526830T
Publication date: 2002-08-20
Inventor:
Applicant:
Classification:
- international: *G06F21/22; H04L29/06;* **G06F21/22; H04L29/06;** (IPC1-7): G06F1/00
- European: H04L29/06C6C
Application number: JP20000572763T 19990928
Priority number(s): US19980102019P 19980928; WO1999US22331 19990928

Also published as:
WO0019324 (A
EP1119813 (A1
EP1119813 (A0

Abstract not available for JP2002526830T
Abstract of corresponding document: **WO0019324**

A system and method for providing a trusted server which controls access to the execution of processes by applying file level extended sensitivity label attributes (202). The attributes are utilized to restrict execution of processes (250) that are requested by comparing the extended attributes (200) in addition to using standard file permission authorization. The system additionally may be used to provide controlled execution of commercially available software.



(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2002－526830
（P2002－526830A）
(43)公表日　平成14年８月20日(2002.8.20)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード(参考)
Ｇ０６Ｆ　1/00		Ｇ０６Ｆ　9/06	６６０Ｄ　５Ｂ０７６ ６６０Ｊ

審査請求　未請求　予備審査請求　有　（全 68 頁）

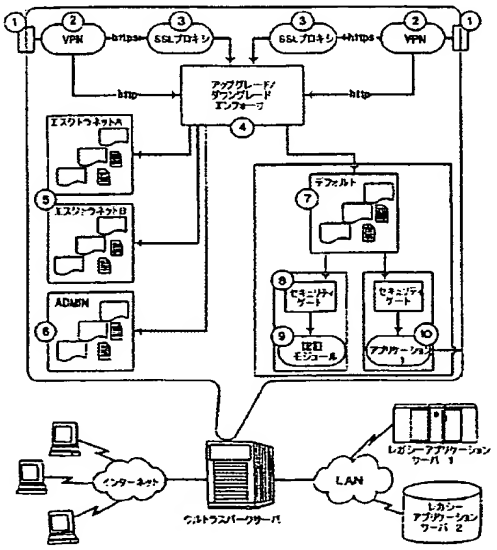
(21)出願番号　特願2000－572763(P2000－572763)
(86)(22)出願日　平成11年９月28日(1999.9.28)
(85)翻訳文提出日　平成13年３月28日(2001.3.28)
(86)国際出願番号　ＰＣＴ／ＵＳ９９／２２３３１
(87)国際公開番号　ＷＯ００／１９３２４
(87)国際公開日　平成12年４月６日(2000.4.6)
(31)優先権主張番号　６０／１０２，０１９
(32)優先日　平成10年９月28日(1998.9.28)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　アーガス　システムズ　グループ，インク．
アメリカ合衆国　61874　イリノイズ，サヴォイ，ウッドフィールド　ドライヴ　1809
(72)発明者　マクナーブ，ポール，　エー．
アメリカ合衆国　61821　イリノイズ，チャンペイン，ブリストル　ロード　2116
(72)発明者　スレイヴィン，パヴェル，　エス．
アメリカ合衆国　61821　イリノイズ，チャンペイン，ターンベリイ　ドライヴ　4009
(74)代理人　弁理士　岡部　正夫　（外10名）

最終頁に続く

(54)【発明の名称】　コンパートメント化された信用コンピュータオペレーティングシステム

(57)【要約】
コンピュータシステムセキュリティと、アクセス、制御、権利、特典が、コンピュータにアクセスするユーザまたは処理にではなく、個々のファイルメンバに指定されるオペレーティングシステム設計を提供する。ファイルレベルを拡張したセンシティビティラベル属性（２０２）を付加することによって、プロセスの実行へのアクセスを制御する信用サーバを提供するためのシステムおよび方法である。属性は、標準ファイル許可認可を使用することに加え、拡張された属性（２００）を比較することによって、要求されたプロセス（２５０）の実行を規制するために使用される。



【特許請求の範囲】

【請求項１】　信用サーバにおいて複数のコンピューティングデバイスからの要求を処理する方法であって、

ａ）入力されるデータオブジェクトの要求を受信する段階と、

ｂ）前記入力されるデータオブジェクトの要求にセンシティビティラベルを指定する段階と、

ｃ）前記データオブジェクトに関連した第１記憶宛先において、拡張された属性を読み出す段階と、

ｅ）前記センシティビティラベルと前記拡張された属性の組み合わせに基づいて、前記入力される要求を該データオブジェクトの第２記憶宛先へ転送する段階と、

ｆ）　前記転送された要求に関連した動作を実行する段階とを有する方法。

【請求項２】　前記入力されるデータオブジェクトの要求に関連する前記第１記憶宛先を決定する段階をさらに有する、請求項１に記載の方法。

【請求項３】　前記拡張された属性は、前記データオブジェクトに付加されたセンシティビティ属性を有する、請求項１に記載の方法。

【請求項４】　前記データオブジェクトは実行されるプロセスである、請求項１に記載の方法。

【請求項５】　前記入力される要求は、前記要求のソースを識別する指示を有する、請求項１に記載の方法。

【請求項６】　前記指示は前記ユーザのＩＰアドレスを表す、請求項５に記載の方法。

【請求項７】　前記要求を解読する段階をさらに有する、請求項１に記載の方法。

【請求項８】　信用サーバ上で実行する商用ソフトウェア製品のデータオブジェクトに制御およびアクセス属性を指定する方法であって、ここで、該商用ソフトウェア製品へのアクセスは前記信用サーバによって限定的に管理され、前記信用サーバは、

ａ）該商用ソフトウェア製品を構成モードで実行する段階と、

b）前記構成モードにある際に、前記商用ソフトウエア製品がアクセスする少なくとも１つのプロセスを決定する段階と、

c）前記データファイルおよびプロセスに指定する少なくとも１つのセンシティビティレベルのための管理者による入力を受信する段階と、

d）該商用ソフトウェア製品の前記プロセスおよびデータファイルに付加する、拡張された属性を決定する段階と、

e）前記受信した管理者のセンシティビティレベルのための前記決定された拡張された属性を、該商用ソフトウェア製品のプロセスおよびデータコンポーネントに付加する段階と、

f）非構成モードで使用するために、前記拡張された属性を記憶する段階と、を実行する方法。

【請求項９】　請求項６の前記信用サーバ上で前記商用ソフトウェア製品を非構成モードで実行する方法であって、さらに、

g）前記信用サーバにおいて、前記商用ソフトウェア製品に関する、要求名とアドレスの指示を備えた要求を受信する段階と、

h）前記商用ソフトウェア製品に関連した前記要求の前記アドレスの指示からセンシティビティレベルを指定する段階と、

i）前記要求から、前記商用ソフトウェア製品のために実行するプロセスの第１場所を決定する段階と、

j）前記第１場所に記憶した、前記商用ソフトウェア製品の前記プロセスに付加された属性を検索する段階と、

k）前記付加された属性を、前記要求に指定された前記センシティビティレベルと比較する段階と、

l）前記検索されたプロセスを、前記付加されたセンシティビティレベルと相関させる、要求された前記プロセスを実行する段階とを有する方法。

【請求項１０】　前記要求されたプロセスを実行する前記段階は、実行する各々のプロセスの該拡張された属性を、前記付加されたセンシティビティレベルと比較する、請求項９に記載の方法。

【請求項１１】　前記プロセスは、前記構成モード中に構成された前記プロ

セスによって定義されたものに制限される、請求項９に記載の方法。

【請求項１２】　前記ユーザのロールを決定するために、前記ユーザの指示は、前記指定されたセンシティビティレベルと共に使用される許可情報を有する、請求項９に記載の方法。

【請求項１３】　前記商用ソフトウェア製品に関連した前記要求を解読する段階をさらに有する、請求項９に記載の方法。

【請求項１４】　オーナー、ワールドおよびグループアクセスに加えて、関連する読み出し、書き込み、削除許可を使って第２のアクセスチェックを実行する、信用サーバのプロセスへのアクセスを制御する方法であって、

ａ）前記信用サーバの管理ユーザアカウントの前記制御形態を区分して、１つの管理アカウントで全ての管理機能を実行できないようにする段階と、

ｂ）前記ファイルシステムの属性を、少なくとも１つのセンシティブレベル属性を含むように拡張する段階と、

ｃ）前記ファイルシステム内の少なくとも１つの記憶場所に記憶されたファイルおよびプロセスの各々に、前記センシティビティレベル属性を指定する段階と、

ｄ）前記システムのプロセスのテーブルを生成する段階であって、前記テーブルは、該プロセスの実行を許可された該ロールとの関係を含む、該段階と、

ｅ）前記ロールに関連した認可を定義する段階と、

ｆ）要求に反応して前記システムが実行するタスクに関連したプロセスの階層を確立する段階と、

ｇ）前記要求に応じて、前記少なくとも１つの記憶場所からファイルおよびプロセスが検索される別の宛先を定義する段階と、

ｈ）入力される、実行するプロセスの要求を受信する段階と、

ｉ）入力されるプロセスの要求にセンシティビティラベルを指定する段階と、

ｊ）前記入力されるデータオブジェクトの要求に関連した、実行するプロセスの第１宛先を決定する段階と、

ｋ）拡張された属性を、前記プロセスに関連した前記第１宛先において読み出す段階と、

l）　前記入力される要求を、前記入力される要求のセンシティビティラベルと前記拡張された属性の組み合わせに基づいて、前記プロセスの別の宛先へ転送する段階とを有する方法。

【請求項１５】　前記プロセスの結果を前記要求者へ送信する段階をさらに有する、請求項１４に記載の方法。

【請求項１６】　要求に応じて、プロセスの制御された実行を許可するための信用サーバコンピューティングシステムであって、

ａ）少なくとも１つのデータパーティション内の拡張された属性を備えた複数のデータオブジェクトを記憶するための記憶手段と、

ｂ）要求を受信し、前記ユーザ要求に応じてプロセスを実行するためのプロセッサ手段と、

ｃ）データオブジェクトの要求に関連したセンシティビティレベルを指定するための指定手段と、

ｄ）前記プロセスと拡張された属性を検索するべくプロセッサを誘導する第１宛先を決定するために、前記要求を翻訳するためのアップグレード・ダウングレードエンフォーサ手段であって、該アップグレード・ダウングレードエンフォーサ手段は、前記属性を前記指定されたセンシティビティレベルと比較し、有益に比較されたプロセスを、実行するべく前記プロセッサへ送る、該手段と、

ｅ）保護された記憶パーティションへのアクセスが必要なプロセスを識別し、センシティブレベルを備えたこれらのプロセスをセキュリティゲート手段へ誘導するプロセッサと、

ｆ）前記センシティビティレベルを受信し、区分された記憶装置からのデータを必要とするプロセスを翻訳するための前記セキュリティゲート手段であって、該セキュリティゲート手段は、前記データセンシティビティレベルが前記受信したセンシティビティレベルと有益に比較される場合に、前記要求されたデータを検索する、該手段とを有する信用サーバ。

【請求項１７】　前記要求は、ユーザのコンピュータ上のネットワークされたユーザから受信される、請求項１５に記載の信用サーバ。

【請求項１８】　前記要求は、前記信用サーバの前記プロセッサによって、

以前の要求の出力として生成される、請求項１５に記載の信用サーバ。

【請求項１９】　システムコンポーネント間で前記要求を暗号化または解読するための暗号化および解読手段をさらに有する、請求項１５に記載の信用サーバ。

【発明の詳細な説明】

【０００１】

本明細書は、本明細書中で援用している、１９９８年９月２８日付けで提出された同時係属米国仮出願番号第６０/１０２、０１９号の優先権に基いており、これを主張するものである。

【０００２】

【発明の属する技術分野】

本発明は、コンピュータシステムセキュリティと、アクセス、制御、権利、特権が、コンピュータにアクセスするユーザまたは処理にではなく、個々のファイルメンバに指定されるオペレーティングシステム設計とに関するものである。本システムは、サーバ上で実行されている処理のアクセスと制御に影響を与えるオペレーティングシステム修正を備えている。

【０００３】

【従来の技術】

以下に示す例により、安全なネットワーキングプラットフォーム（例えば、インターネットのためのもの）の重要性が強調される。１９８８年１１月前半、Ｂｅｒｋｅｌｅｙ　ＵＮＩＸ（登録商標）のバージョンを実行しているＶＡＸおよびＳｕｎ－３コンピュータに侵入する自己複製プログラムがインターネット上に放たれた。このプログラムは、これらのコンピュータのリソースを不当に利用して、インターネットに接続している他のコンピュータを攻撃した。このプログラムは数時間で全米中に広がり、存在する６０，０００のインターネットホストの内６，０００のホストに感染した。この時、インターネットはまだ科学者どうしの間でのメール交換に独占的に使用されているだけであった。企業のインターネットサービスが静止したウェブページ、メールゲートウェイなどに限定されていた時、セキュリティ手段は主に、電子販売およびマーケティング情報を公共に確実に提供するために必要とされていた。このようなセキュリティがインターネットサーバを攻撃から保護することに失敗すると、企業では、インターネットを視認することが一時的に中断され、重要でないサービスしか受けられず、全体的であるが、致命的ではない管理上の問題が引き起こされる。

【０００４】

今日では、膨大スケールの公共および企業サービスをインターネットに頼る人や企業はますます増加する一方である。企業は、経費の削減と競合性の拡大を目的として、公共インターネットサービス上で商用アプリケーションを急速に展開している。これらの統合されたアプリケーションは、コストを削減し、視認性を向上させながら、ビジネスプロセスにかけて、速くて便利なサービスと価値のある顧客管理を提供する。

【０００５】

【発明が解決しようとする課題】

しかし、インターネットのためのトランザクション技術は発展したが、セキュリティの突破口から生じる潜在的なダメージは、企業が考慮するべき重大な要素となった。データの盗難や破壊、ネットワークサービスの拒否は、企業の利益に明確な打撃を与える。

【０００６】

インターネット上で伝送されるミッションクリティカルなサービスへの増加する依存には、外部の人物が、重要な内部データへのパイプラインをインターネットを介して開いてしまうという危険が付きまとう。ファイアウォールの後ろにあるアプリケーションおよびデータベース情報とのインタラクションが可能になったウェブを採用する前に、ウェブサイトのコンテンツが攻撃の危機に晒されてしまうかもしれず、今日では、トランザクショナルなインターネットアプリケーションを実現するために必要な接続性が、これらの重大な企業リソースを攻撃し易いものにしてしまう。現在インターネットサーバは、ミッションクリティカルなサービスを企業に提供し、プライベートおよび公共のシステムとデータを接続する。例えば、この新規のビジネスモデルの下では、以前は最大でも公的に利用可能な情報のみをインターネットに提供していたシステムが、現在では、世界のあらゆる場所から、銀行預金情報や、コンピュータハッカーのトランザクション記録といった機密データへ続く潜在的なドアとなっている。

【０００７】

全てのコンピュータシステム上で、特定のシステムプログラムまたはユーティ

リティに、通常はシステムによって強いられるセキュリティ制約をバイパスする機能が付与される。例えば、システムディスク上の全てのファイルのバックアップを作成するために、管理者は、通常はこうしたアクセスを許可されないにも関わらず、ディスク上の全てのファイルを読み出せるバックアッププログラムを実行できなければならない。これ以外の協力なプログラム、例えば、システムをシャットダウンするプログラム、新規のユーザを作成するプログラム、損傷したファイルシステムを修正するプログラムも注意深く制御されるべきである。標準のＵＮＩＸシステム上では、ルートまたはスーパーユーザと呼ばれる１人のユーザＩＤが全てのセキュリティ規制および制限をバイパスすることができるオペレーティングシステムが設計されてきた。Ｗｉｎｄｏｗｓ（登録商標）　ＮＴシステムでも、「システム」アカウントと「管理者」アカウントを使用して、同様の脆弱性を示す。

【０００８】

このため、あらゆる規制された機構を使用するために必要なユーティリティを、ルートまたは管理者として実行しなければならない。これは例えば、システムをシャットダウンするためにバックアッププログラムを利用することができ、新規のユーザを作成するためにシャットダウンプログラムを利用することができ、また、新規のユーザを作成できるプログラムを、システム上の全てのファイルを読み出すために利用することができるということである。従って、任意の管理プログラムが利用可能なバグを含んでいる場合には、システム上であらゆることを実行するためにそのプログラムを使用することができる。

【０００９】

限定された権利のみをプログラムに付与に対する標準ＵＮＩＸの不能さは、このシステムの唯一の弱点ではない。ＵＮＩＸでは、１つのプログラムが別のプログラムを開始する際に、ユーザＩＤと最初のプログラムの許可によって新規に作成されたプログラムが実行される。これは、ルートプログラム内のバグを利用できる悪質なユーザが、インタラクティブなルートセッションを開始できてしまうということである。ユーザがルートを実行している場合、そのユーザが実行する全てのファイルがシステム上で無制限の特権を持つ。ユーザはあらゆるファイル

の作成、修正、削除を行うことができる。ユーザは選択するあらゆるネットワークパケットを追加的に送受信することができ、またネットワーク上の全てのパケットを妨害する機能を持つため、同じネットワーク上にある他者のあらゆる２つのホスト間のトラフィックを見ることができてしまう。

【００１０】

ファイアウォール、侵入検出、暗号化、ユーザ認証は、ペリメータおよび通信セキュリティの要素を提供するが、これらは１つだけでは、高度のセキュリティ保証を必要とするインターネットベースのアプリケーションにとっては不十分である。オンラインバンキング、オンライン株取引、センシティブなデータベースへのアクセス、政府の税処理、電子商取引、ジャストインタイムの製造業のようなミッションクリティカルなプロセスは、自分を露出して危機に晒すことなく内部サーバおよびデータベースへのアクセスを提供できるシステムを必要とする。これらは、従来のセキュリティ手段では解決できないセキュリティ問題である。

【００１１】

従来のセキュリティ手段は、システムへのアクセスを制限するが、システムへの、またはシステムからの動作を制限することはできない。これらの手段は、悪意を持った認可されたユーザがアプリケーションまたはオペレーティングシステムソフトウェアに存在する未発見のホールを発見し、これを利用してしまうという状況においては役に立たない。

【００１２】

一般に、これらの製品は、認可および認証されたユーザは信用できるユーザであるという誤った考えの上で動作する。例えば、有効な口座番号とＰＩＮを持った悪質な銀行顧客がいるとする。従来のセキュリティ手段は、この人物を認可された合法なシステムユーザであると認識してしまう。インターネットサーバへのアクセスを一旦許可されれば、この口座の所有者はサーバを攻撃し、これをバックエンドデータベースおよび金融サーバへエントリするための橋頭堡として使用することができるのである。

【００１３】

数名の有名なコンピュータ産業アナリストが行った研究では、セキュリティマ

ネージャが恐れるシステムの完全性と安全性への最も顕著な脅威は、企業内の認可された人物による悪質ないたずらと誤用であると示されている。これらの統計は、有効なセキュリティソリューションが、システムの使用を許可された内部関係者およびその他の人物から、また、熟達した知識豊富な攻撃者からの的確な攻撃からシステムを保護する問題を検討したものでなければならないことを示している。

【００１４】

ファイアウォールは、ホストシステムおよびサービスへのアクセスを制限することにより、攻撃に対する必要なペリメータディフェンスのラインを提供する。しかし、ファイアウォールは、アクティブコンテンツを生成したり、トランザクション指向のサービスを実現するアプリケーションの危険を適切に減少させることはできない。この用語が意味するように、ファイアウォールは、対立的な環境（インターネット）から友好的な環境（ローカルな企業ネットワーク）までの全体的なアクセスを規制するものである。新しいトランザクションベースのインターネットサービスのパラダイムは、友好的環境と非友好的環境の間の境界線が明確でない場合には、これらの「ペリメータ」ディフェンスの有効性を減少させてしまう。

【００１５】

ファイアウォールは、その「中」に入る全てのネットワークおよびリソースへの幅広いアクセスを制御する。ユーザからのパケットがファイアウォールをトラバースし、内部ネットワークへのエントリを認可されてしまえば、ファイアウォールは、特定のリソース、または最悪の場合セキュリティデータ自体へのアクセスまたは修正を阻止することはできない。インターネットベースのトランザクションシステムについては、セキュリティ機構が、個々のユーザのプロファイルに基づいて、特定のウェブページ、アプリケーション、データベースへのアクセスを提供または拒否できなければならない。

【００１６】

セッションの暗号化と通信セキュリティは、情報が伝送中である場合に顧客のプライバシーを保護することができるが、商用トランザクションサーバに常駐し

ているデータを保護することはできない。一旦伝送または解読されてしまった後では、伝送途中では保護されていた同一の情報が、サーバ上に記憶されて攻撃の危機に晒されてしまう。

【００１７】

同様に、暗号化キーは、インターネットサーバ上に記憶されている間、開いたままの危険な状態に保たれる。暗号化キーがマシン生成された６４文字のストリングであるシステムを考える。このような暗号を解読することは侵入への気力を挫くタスクに思われるかもしれないが、ユーザがこれらのストリング（または、これらを生成するために使用されるランダムナンバーのアルゴリズム）が常駐するシステム上のファイルにアクセスできれば、暗号化スキームは完全に失敗する。

【００１８】

ユーザ認証機構についても同様のことが言える。悪質なユーザがペリメータディフェンスを破ってしまえば、このユーザはキーを入手し、偽ＩＤを受諾するよう認証システムを騙すことができ、システムおよび全てのリソースが無防備な状態にされてしまう。

【００１９】

侵入検出はシステム上への攻撃に反応するツールである。これは、悪質な意図に関連した動作の公知のパターンを検出するシステムの機能に依存したものである。このような検出システムは新規のものには無効であることが明白である。例えば、サーバ内のこれまで知られていないシステムバグを利用するために明らかに無害のパケットを使用した攻撃には、恐らくこのシステムは気付かないであろう。侵入検出機構は純粋に受身であり、最初の侵害の発生を防止する上では全く何もできない。セキュリティホールが使用されてしまうと、アプリケーションとオペレーティングシステムファイルが開かれて破壊され、これにより、攻撃者は他の、未検出のセキュリティホールを空けることができてしまう。さらに、システム監査トレイルへの自由なアクセスを手に入れた攻撃者は、多くの場合、彼らの不法侵入のシステムトレースを消し去ることができ、攻撃が最も深刻である場合は、侵入検出機構を事実上無効にすることができる。

【００２０】

ほとんどのＩＳと企業マネージャは、既に毎日のシステムオペレーションを維持するのに精一杯であり、新規技術と適切なシステムセキュリティを採用するための顕著なバリアと直面している。そのため、システムのセキュリティのアップグレードを求めているマネージャは、セキュリティパフォーマンスについてのベンダーからのクレームに依存するしかない場合が多い。新しいソフトウェアがリリースされ、既存のソフトウェアへアップグレードが不可避になると、通常、ＩＳプロフェッショナルは、ベンダーが製品のセキュリティに力を注いだと推測する。セキュリティシステムの失敗の潜在的な実現を見れば、マネージャが、個別に評価、テスト、証明を行ったセキュリティソリューションに注目することは非常に重要である。

【００２１】

信用オペレーションシステムは、全体的な設計の評価、ソースコードの統合性と信頼性の証明、システマチックな独立したペネトレーション評価を受ける。最も高く評価される評価ツールの１つに、国際的に認識された、ＩＴセキュリティ製品を評価、テスト、証明するための標準セットである情報技術セキュリティ評価基準（ＩＴＳＥＣ）がある。独立した本体によって実施されるＩＴＳＥＣ証明は、製品のセキュリティ機能について受けたクレームが確かであるという自信をエンドユーザに与える。さらに、この証明は、これらのクレームが、保証の所定レベルに対してテスト済みであり、ベンダーが高い専門技術と、安全性への強い責任を持っていること示す。

【００２２】

従って、ネットワークサービス用の安全なプラットフォームを提供するためにこれらのコンポーネントが完全に統合されており、ユーザがシステムをインストールした直後に、そのセキュリティ機能を発揮し、アプリケーションとサーバを保護されたパーティション内にインストールすることができるシステムを提供することが望ましい。オペレーティングシステムの全て（その他のあらゆる従来の信用オペレーティングシステム）を交換するために管理者を必要とするのではなく、望ましいシステムの信用オペレーティングシステムは、システムのアップグ

レードとしてインストールされた拡張を有する。これにより、内在するオペレーティングシステムＡＰＩとの１００％の互換性を維持することができ、また、通常このタイプのシステムに関連する、経費と時間のかかる統合作業を大幅に縮小することができる。

【００２３】

【課題を解決するための手段】

本発明の目的は、アクセスが厳密に制御され、要求に反応する必要がある動作のみを許可するべく処理が規制される、ファイアウォールまたは情報サーバ上で使用するための安全オペレーティングシステムを提供することである。また本発明の別の目的は、管理プロセスが制御され、ローカルマシンのみについて実行されるため、ネットワークユーザが、ローカルネットワークの外からシステムの管理機能へアクセスしたり、これを修正することができないサーバシステムを提供することである。さらに、本発明の別の目的は、システムからデータを要求するためのユーザの認可が、要求を行っているユーザに確立されたロールと比較されることである。また、本発明の目的は、ユーザによる要求は、事前定義されたプロセスしか開始することができず、プロセスを実行する認可が各プロセス段階において確認され、プロセスが権利または別の後続するプロセスへのパス権利を引き継がないことである。本発明のさらに別の目的は、異なるユーザからの同じアイテムへの要求は、ユーザが異なる場所へと誘導され、そこでそれぞれ異なる結果を得られることである。本発明のまた別の目的は、ファイル許可が、拡張された属性が各ファイルおよび実行可能なプロセスに指定されるように修正され、システムによって要求を受信する度に、これらの属性が検査されることである。

【００２４】

このオペレーティングシステムと協働するべく、保護部分をこの方法で動作するように修正したウェブサーバが採用されており、オペレーティングシステムの非エンベッド部分と選択的にインターオペレートできればさらに望ましい。

【００２５】

本発明の別の目的は、入力される通信のＩＰアドレスに基づいてセンシティビティ層を指定することである。本発明のさらに別の目的は、リソースへのアクセ

スを許可する前に、センシティビティ層をチェックすることで、使用可能なプロセスおよびリソースへのアクセスを規制することである。本発明の別の目的は、ウェブユーザに、要求されたプロセスと、受信した認可レベルとによってアクセスが制限される第２コンピューティングリソースから、保護されたリソースへのアクセスを可能にすることである。

【００２６】

本発明のさらに別の目的は、ファイアウォールや暗号化プロセスのような従来のセキュリティコンポーネントが、商用サーバへの攻撃を確実に打破できるように修正され、また、基本のセキュリティ層がオペレーティングシステムレベルに下げられ、ファイルシステム、デバイス、プロセスへのアクセスについての決定が行われ、効率性と柔軟性を以て動作している間にはセキュリティをバイパスすることができないようにすることである。

【００２７】

本発明は、ファイアウォールや侵入検出ツールのような従来のセキュリティ機構の代わりではなく、むしろ、全てのオペレーションレベルにおいてデータとアプリケーションの統合性を確実にするためのセキュリティの追加層を提供する。本発明は、信用サーバにおいて複数のコンピューティングデバイスからの要求を処理する方法であり、入力されるデータオブジェクトの要求を受信する段階を有し、入力されるデータオブジェクトの要求にセンシティビティラベルを指定する段階をさらに有し、データオブジェクトに関連した第１記憶宛先において、拡張された属性を読み出す段階をさらに有し、センシティビティラベルと拡張された属性の組み合わせに基づいて、入力された要求をデータオブジェクトの第２記憶宛先へ転送する段階をさらに有し、転送された要求に関連した動作を実行する段階をさらに有する。

【００２８】

さらに、信用サーバ上で実行する商用のソフトウェア製品のデータオブジェクトに制御およびアクセス属性を指定する方法であり、ここで、商用ソフトウェア製品へのアクセスは信用サーバによって規制的に管理され、信用サーバは、商用ソフトウェア製品を構成モードで実行する段階と、構成モードにある際に、商用

ソフトウエア製品がアクセスする少なくとも１つのプロセスを決定する段階と、データファイルおよびプロセスに指定する少なくとも１つのセンシティビティレベルのための管理者による入力を受信する段階と、商用ソフトウェア製品のプロセスおよびデータファイルに付加する、拡張された属性を決定する段階と、受信した管理者のセンシティビティレベルのための決定された拡張された属性を、商用ソフトウェア製品のプロセスおよびデータコンポーネントに付加する段階と、非構成モードで使用するために、拡張された属性を記憶する段階とを実行する方法が提供される。

【００２９】

構成モードに続いて、信用サーバ上で商用ソフトウェア製品を非構成モードで実行する方法であり、さらに信用サーバにおいて、商用ソフトウェア製品に関する、要求名とアドレスの指示を備えた要求を受信する段階を有し、商用ソフトウェア製品に関連した要求のアドレスの指示からセンシティビティレベルを指定する段階を有し、要求から、商用ソフトウェア製品のために実行するプロセスの第１場所を決定する段階を有し、第１場所に記憶した、商用ソフトウェア製品のプロセスに付加された属性を検索する段階を有し、付加された属性を、要求に指定されたセンシティビティレベルと比較する段階を有し、検索されたプロセスを、付加されたセンシティビティレベルと相関させる、要求されたプロセスを実行する段階を有する方法が提供される。

【００３０】

オーナー、ワールドおよびグループアクセスに加えて、関連する読み出し、書き込み、削除認可を使って第２のアクセスチェックを実行する、信用サーバのプロセスへのアクセスを制御する方法であり、信用サーバの管理ユーザアカウントの制御形態を区分して、１つの管理アカウントで全ての管理機能を実行できないようにする段階を有し、ファイルシステムの属性を、少なくとも１つのセンシティブレベル属性を含むように拡張する段階をさらに有し、ファイルシステム内の記憶場所に記憶されたファイルおよびプロセスの各々に、センシティビティレベル属性を指定する段階をさらに有し、システムのプロセスのテーブルを生成する段階をさらに有し、テーブルは、プロセスの実行を許可されたユーザロールとの

関係を含んでおり、ユーザロールに関連したユーザ認可を定義する段階をさらに有し、ユーザ要求に反応してシステムが実行するタスクに関連したプロセスの階層を確立する段階をさらに有し、ユーザ要求に応じて、記憶場所からファイルおよびプロセスが検索される別の宛先を定義する段階をさらに有し、入力される、データオブジェクトの要求を受信する段階をさらに有し、入力されるデータオブジェクトの要求にセンシティビティラベルを指定する段階をさらに有し、入力されるデータオブジェクトの要求に関連した、第１宛先を決定する段階をさらに有し、拡張された属性を、データオブジェクトに関連した第１宛先において読み出す段階をさらに有し、入力される要求を、入力される要求のセンシティビティラベルと拡張された属性の組み合わせに基づいて、別の宛先へ転送する段階をさらに有する方法が提供される。この方法はさらに、同じ方法で処理されるか、要求者に出力を送る別のプロセス要求を最終的に有する、要求された出力を生成する。

【００３１】

要求に応じて、プロセスの制御された実行を許可するための信用サーバコンピューティングシステムであり、少なくとも１つのデータパーティション内の拡張された属性を備えた複数のデータオブジェクトを記憶するための記憶装置を有し、要求を受信し、ユーザ要求に応じてプロセスを実行するためのプロセッサ手段をさらに有し、データオブジェクトの要求に関連したセンシティビティレベルを指定するための指定手段をさらに有し、プロセスと拡張された属性を検索するべくプロセッサを誘導する第１宛先を決定するために、要求を翻訳するためのアップグレード・ダウングレードエンフォーサ手段をさらに有し、アップグレード・ダウングレードエンフォーサ手段は、属性を指定されたセンシティビティレベルと比較し、有益に比較されたプロセスを、実行するべくプロセッサへ送り、保護された記憶パーティションへのアクセスが必要なプロセスを識別し、センシティブレベルを備えたこれらのプロセスをセキュリティゲート手段へ誘導するプロセッサをさらに有し、センシティビティレベルを受信し、区分された記憶装置からのデータを必要とするプロセスを翻訳するためのセキュリティゲート手段をさらに有し、セキュリティゲート手段は、データセンシティビティレベルが受信した

センシティビティレベルと有益に比較される場合に、要求されたデータを検索することを特徴とする信用サーバが提供される。

【００３２】

【実施例】

本発明は、安全なビジネス処理のための完全統合ソフトウェアファンデーションである。本発明は、シームレスで安全なシステムに様々なセキュリティ技術を採用している。そのコンポーネントと修正形は、オペレーティングシステムセキュリティ拡張、ネットワークパケット管理修正、アップグレード/ダウングレードエンフォーサ（ＵＤＥ）、セキュリティゲート、信用管理ユーティリティ、拡張されたセキュアシェル（拡張ＳＳＨ）、認証モジュール、セキュアＣＧＩモジュール、ネットワーク層暗号化（ＶＰＮ）、セキュアソケット層暗号化（ＳＳＬ）の使用を備えている。

【００３３】

以下に示す用語は、本願明細書の好ましい実施例の説明と共に有益である。

アドバンスド・セキュア・ネットワーキング（ＡＳＮ）：　パケットが属するコンパートメントまたはパーティションを表示するために、入力パケットの各々にラベルを指定するネットワークインタフェースに関連したセキュリティコンポーネントである。

【００３４】

監査証跡：　処理の文書証拠を総合的に提供する１組の記録である。監査証跡により、オリジナルのトランザクションから関連する記録やレポートへ送信された、または逆に、記録やレポートからそのコンポーネントソース・トランザクションへ送信されたイベントの追跡が可能になる。

【００３５】

認証：　クレームされた識別の有効性を確立する。

【００３６】

証明：　特定のコンピュータシステムの設計と実装が特定の１組のセキュリティの条件に見合う範囲を確立するための、システムの障害を技術評価する承認/アクレディテーション処理。

【００３７】
共通ゲートウェイインタフェース（ＣＧＩ）：　ウェブサーバ上で実行されているプログラムがウェブクライアントと通信する方法を指定するプロトコル。

【００３８】
コンパートメント：　アクセスを承認する前に、相関のために特定のアクセスコードが必要なオペレーティングシステムによって制御されるシステムの部分であり、パーティションとも呼ばれる。

【００３９】
データの統合性：　計算されたデータがソースドキュメント内のものと同一であり、不慮の、または故意による変更または破壊に晒されていない状態のことである。

【００４０】
任意アクセス制御（ＤＡＣ）：　属するサブジェクトおよびグループの識別に基づいてオブジェクトへのアクセスを規制する手段である。特定のアクセス許可を持ったサブジェクトは、その許可を（おそらく間接的に）別のサブジェクトへと送ることができるため、（命令アクセス制御によって規制されていない限り）制御は任意であると考えられる。

【００４１】
ハイパーテキスト・マークアップ言語（ＨＴＭＬ）：　テキストに構造を付加するための、ＳＧＭＬベースの標準である。ＨＴＭＬは、ウェブ上の大多数のドキュメントで使用されているマークアップ方法である。

【００４２】
インターネットプロトコル（ＩＰ）：　デバイスを個々に識別し、相互に通信するための、インターネット上でのデバイスの接続方法を指定する標準である。

【００４３】
ＩＴＳＥＣ（情報技術セキュリティ評価基準）：　情報技術セキュリティ製品を評価、テスト、証明するための、国際的に認識された標準セットである。

【００４４】
最下位の特権：　システム内の各サブジェクトに、認証されたタスクのパフォー

マンスに必要とされるよりも多くの特権（それ以上高いクリアランス）を与えてはいけないという原則である。この原則を適用することで、事故、エラー、非認証の使用により生じるダメージを制限することができる。

【００４５】

命令アクセス制御（ＭＡＣ）：　オブジェクト内に含まれる情報のセンシティビティ（ラベルが示すもの）と、このようなセンシティビティの情報にアクセスするべく特定の要求に与えられた正規の認証（クリアランス）とに基づいて、オブジェクトへのアクセスを規制する手段である。

【００４６】

マルチレベルセキュア：　知る必要があり、特定の正しいセキュリティクリアランスを有するユーザによる、異なるセンシティビティを持った様々な情報のセットへのアクセスを許可するが、ユーザが認可を持っていない情報へのアクセスを得ることは阻止するシステムのクラスである。

【００４７】

パケットラベリング：　要求処理の許可レベルに関連する情報を、入力または出力データグラムに付加する処理である。

【００４８】

セキュアソケット層（ＳＳＬ）：　ウェブユーザにセッション層の暗号化を提供する機構である。

【００４９】

セキュリティゲート（ＳＧ）：　個別のパーティション内で動作しているアプリケーションまたはユーティリティ間の制限された、安全な通信を可能にするソフトウェアコンポーネントである。

【００５０】

センシティビティラベル（ＳＬ）：　要求のセキュリティレベルを示し、オブジェクト内のデータのセンシティビティ（例えば、類別）を表記する情報である。センシティビティラベルは、命令アクセス制御決定の基準として使用される。

【００５１】

システムネットワーク・アーキテクチャ（ＳＮＡ）：　特定のネットワークハー

ドウェア構成である。

【００５２】

信用コンピュータシステム：　サービスの拒否、データ盗難、または悪質な行為による変造の心配をすることなく、センシティブ情報または類別された情報を処理するために依存できる、適切なハードウェアとソフトウェアの統合性の基準を採用したシステムである。

【００５３】

ユニフォーム・リソース・ロケータ（ＵＲＬ）：　所与のオブジェクトの位置と、その検索に使用されるプロトコルを識別するためにウェブ上で使用されているアドレス指定システムである。

【００５４】

アップグレード／ダウングレードエンフォーサ（ＵＤＥ）：　入力される要求の各々を調べ、どのアプリケーション（ウェブサーバなど）でそれを扱うかを決定する機能を果たす、本発明のコンポーネントである。

【００５５】

図1に示す本発明の信用サーバは、キーコンポーネントの操作に影響を与えるように、オペレーティングシステムに修正を加える必要がある。以下で説明する信用オペレーティングシステムのキーコンポーネントには、１）プロセス、２）ファイルシステムオブジェクト（デバイス、ディレクトリ、ファイルなどを含む）、３）インタープロセス通信メッセージ（パケット、共用メモリなどを含む）がある。標準システムではこれらの各々が様々なセキュリティ属性を持っており、これらのセキュリティ属性はＯＳ自体によって作成、管理、使用される。プロセスがファイルシステムオブジェクトにアクセスしようとすると、ＯＳがそのプロセスの様々な属性をオブジェクトの属性と比較し、アクセスを許可または拒否する。プロセスが通信メッセージを送信または受信すると、ＯＳは、プロセスがそのメッセージの送信および/または受信を認められていることを確認する。ファイルの作成時またはメッセージの生成時のようにオブジェクトが作成される場合、ＯＳは、新規のオブジェクトに適切な属性を付加するべく機能する。

【００５６】

信用サーバシステムは、ＯＳコンポーネントの各々にセキュリティ属性をさらに付加することにより、また、新規の属性を使用するべくセキュリティチェックを拡張することにより、この標準機構を２つの方向に拡大している。３種全てのコンポーネントに追加されたセキュリティ属性は、「センシティビティラベル」２０２またはＳＬである。図２は、ファイルに付加された拡張された属性を示し、図３は、システム上で処理されるプロセスまたはパケットに付加された属性を示す。図３は、この構造の1部分である属性タイプを表に示したものである。図４はこの構造の一部分である属性タイプを表に示したものである。標準のセキュリティ機構とは違い、ＳＬ２０２は命令として、つまり、ユーザの制御下にないものとして設計されている。つまり、ユーザはファイルを所有していても、そのような情報を入手するべく事前に許可されていなければ、そのユーザがアクセス可能なファイルや内容、またはコピーさえも作成することができない。ＳＬは、次に示すいくつかの形で関連することができる。１）同一である、２）他方よりも「大きい」（優位である）、３）「ディスジョイント」である（つまり、どちらも大きさが同じである）。単純な類推は、ＳＬの関係を説明する上で役に立つ。多くの部門と管理レベルを持つ大企業では、管理者の階層構成がある場合がある。多くの場合、ある従業員は、この階層において別の従業員の「上」または「下」として表すことができる。しかし、ある部門のスーパーバイザは別の部門の従業員に対しては何の権限もないため、互いにタスクを与え合うことはできない。実際、例えば経理部門のようなある部門の最下にある従業員が、別の部門の最高幹部がアクセスを拒否される情報にアクセスできることがある。

【００５７】

プロセスは実行プログラム、つまり、書き込まれ、ファイルに記憶され、システムによって「実行可能」であると判断されるコンピュータプログラムの例である。多くの場合、コンピュータプログラムは、例えば、ネットワークブラウザプログラムがワードプロセッサプログラムまたはモデムソフトウェアパッケージの実行を開始した際といった、ある段階において別のプログラムを「呼び出す」または「実行する」ように書かれている。プロセスがこの要求を行うと、プロセスがそのプログラムを実行できるかどうか確認するために、ＯＳがそのプロセスの

属性を、プログラムが記憶されているファイルの属性と比較する。使用可能なプログラムに対して制御を強化するために、ＯＳは、信用サーバシステムの追加のセキュリティ属性を使用する。信用サーバシステムは、標準のユーザおよびグループ識別子に加え、プロセスを実行しているユーザが、要求したプログラムにアクセスまたは実行できるかどうかを調べるために用いる「認可データベース」をＯＳに追加した。

【００５８】

あらゆるシステム上で、プログラムによっては、ある特定の作業を実行するために、いくつかのセキュリティをバイパスする必要があるものもある。例えば管理者は、たとえ普段は全てのファイルにアクセスできなくても、システムのバックアップを作成する際には、全てのファイルを読み出し、その各々をテープまたはディスクに書き込むべくあるプログラムを実行できる必要がある。このような状況下で、プロセスに特定のセキュリティ機構をバイパスさせるために、プロセスの「特権」属性が使用される。特権はプログラムの実行可能ファイルに記憶されるため、そのプログラムが実行されると、これを実行しているプロセスが必要な特別の機能を持つ（本システムではこの特権を「特権」と呼ぶ。）。

【００５９】

本発明の信用サーバシステムは、従来の認可および特権に加えて、開始特権セット以外に、少なくとも１組の特権を、「特権認可セット」２２０と呼ばれる追加の認可リストと共にプログラムファイルに付加する概念を追加した。プログラムを実行すると、そのプログラムを実行しているユーザが1つまたはそれ以上の特権認可を有する場合、プロセスに開始特権と「認可特権」が与えられる。これにより、管理者は、ユーザが単にプログラムへのアクセスを許可または拒否されるだけでなく、ユーザが特定のセキュリティ規制をバイパスするより広範な機能を持ちながらプログラムを実行できるようにプログラムを設定することができる。この機構は、プログラム自体にではなく、ディスクに記憶されたそのプログラムファイルのコピーに適用されるため、ソースコードへのアクセスを持たない、ソフトウェアの商用のバイナリコピーに加えることができる。

【００６０】

信用サーバシステムの信用サーバは、各プロセスに最小２５４および最大クリアランス（ＳＬ）２５６を追加した。この追加の属性は、特定の特権を制限するために使用される。特権機構を使用し、ＳＬを提供する別のシステムでは、ＳＬチェックを無視する特権を特定の範囲に限定することはできない。そのため、複数のＳＬを使用して特別のプログラムを実行する必要がある場合には、このプログラムに、全てのＳＬチェックを無効にする旨をシステムに伝える特権が与えられる。クリアランス範囲２５４、２５６を提供することにより、また、ＳＬ無効特権の範囲を制限するためのチェックを加えることにより、信用システムは、サイトに、特別な「マルチレベルオペレーション」を扱いながら、各々を別々に保つ機能を持った多数の特別なプログラムを実行させることができる。

【００６１】

プロセスが通信チャネルまたはネットワークを介して情報を伝送する場合、信用サーバはＯＳを、プロセスのセキュリティ属性がパケットに付加されるように変更する。同じマシン上の別のプロセスと通信する場合には、そのパケットへのアクセスを宛先プロセスに与える前に、セキュリティ属性のチェックを行うことができる。そのため、ＯＳは、ＳＬのような様々なセキュリティ属性に基づいて、プロセス上のセキュリティを実行することができる。パケットがネットワークインタフェース上に送信されると、信用サーバは、セキュリティ情報をネットワークパケット内に組み込むことができるため、受け側のシステムは、そのパケットが到着した際にこれを正しく設定することができ、また、パケットへのアクセスをプロセスに許可する前に、セキュリティを正しくチェックすることができる。セキュリティ情報を組み込まれていないパケットがネットワークから届いた場合、または、組み込まれた情報を全てを無視するように信用サーバシステムが構成されている場合には、システムが、システム管理者によって構成された内部テーブルに基づいてデフォルトセキュリティ属性を追加する。従来技術では、デフォルトセキュリティ属性のセットを決定するために、このようなテーブルが、パケットのソースホストのＩＰアドレスと、パケットが届けられたネットワークインタフェースを使用した。信用サーバはこれに、インタフェース、ソースネットワーク/サブネット、ソースＩＰアドレスと共に、ポート番号（ＨＴＴＰ、ＦＴ

Ｐ、ｔｅｌｎｅｔなどの様々なネットワークサービスを特定する）および/またはプロトコル（ＴＣＰまたはＵＤＰなど）を使用できる機能を追加した。さらに、信用サーバでは、管理者は、システムから送信される、また、システム内に受信されるパケットに個別の規則を設けることできる。これらの規則は、入ってくる、ラベル付けされていないパケットにデフォルト情報を提供するためだけでなく、パケットを特定のネットワークインタフェースに、または特定のホストまたはネットワークに送受信を認可すべきかどうかを決定するために使用される。このシステムのプロセスまたはコンポーネントは、ソフトウェアコンポーネントを用いて実現することが、あるいは、プロセスを組み込んだマイクロプロセッサを活用することができる。

【００６２】

ＵＮＩＸ実装の好ましい実施例では、信用サーバシステムは、デフォルトｉノード構造情報に加えて、既に記憶されている、ファイルに関連した属性ラベル情報を検索するためにリンクを設けた、本発明のカーネルプロセスを実行するコンピュータを備えている。別の実施例では、ｉノード構造を、記憶装置の別の部分を（パーティション）に記憶されている別の情報を見ることなく、本発明のシステムの処理ルーチンがアクセスできるようにラベル情報を直接包含するべく修正している。カーネルは、プロセスが記憶装置からファイルを呼び出す毎に、このラベル情報を検索するように適合される。ユーザの基本の権限と許可がファイルの実行を許可し、システム内に拡張した属性がユーザにそのレベルの情報へのアクセスを許可する場合には、このラベルにより、プロセッサは、その参照ロケーションに記憶されたファイルを直接検索することができる。システムは、プロセスと認可の関係を記憶するための記憶装置手段と、ローカルプロセッサまたは遠隔地にいるユーザから受信した要求を翻訳するためのプロセッサ手段とを備えており、このプロセッサ手段は、リソースへのアクセス可能性を決定するための、また、ユーザのデータの要求を適切な場所へ誘導するためのアップグレード/ダウングレードエンフォーサと、レガシーアプリケーションと要求プロセスの間の適切な通信を規制およびチェックするためのセキュリティゲートとを装備している。

【００６３】

図１およびプロセス図を参照すると、パケットがネットワークインタフェース１に到着すると、アドバンスト・セキュア・ネットワーキング（ＡＳＮ）コンポーネントがこれに、属するコンパートメントを表示したラベルを指定する。コンパートメントは、そのＩＰアドレスを介してアクセス可能なデータを示している。ラベルはインターフェースまたはソースホストアドレスに基づき指定される。ネットワーク層暗号化を用いてパケットが認証されない限り、ホストアドレスは絶対に信用されない。アップグレード/ダウングレードエンフォーサ４は、指定されたラベルを使用して、パケットの保護方法を確立し、適切な宛先を決定する。

【００６４】

ＵＤＥ４の役割は、入力される要求の各々を調べ、これを適切なサービスへ転送することである。ＵＤＥは密接に統合された信用プログラムであり、他のプロセスやプログラムとは違って、異なるセキュリティパーティション間でパケットを通過させることができる。ＵＤＥは決定をする上で次の３つの要素を調べる。ＡＳＮが（ＩＰアドレスおよび/またはネットワークインタフェースに基づいて）パケットに付加したラベル、要求されたＵＲＬ、ユーザ認証モジュールの認証の試みが成功した結果現れたあらゆる「認証されたクッキー」。

【００６５】

セキュリティゲート８（図1を参照）プログラムは、２プロセス間、またはプロセスとネットワークインタフェース間の制限された通信を認める特別なプログラムである。その構造ファイルは、宛先ＳＬとポートと共に、ソースＳＬとポートを指定する。一般的な構造では、ソースおよび宛先ＳＬはディスジョイントであり、つまり、両端は相互に作用することが決してできない。セキュリティゲートプログラムには、両方よりも大きなＳＬが与えられている。また、ＳＬセキュリティチェックを無視する特権と共に、両エンドポイントを含むＳＬ範囲も与えられるが、その範囲内に含まれるＳＬのみに限定される。

【００６６】

ＵＤＥ（アップグレード／ダウングレードエンフォーサ）プログラムは、セキ

ュリティゲートよりも複雑である。入ってくるパケット（システムに到達した際に、セキュリティ属性を指定されている）を、そのＳＬを修正した形で別のポートへ送信することができる。ＵＤＥは、どのアクセスを許可するか決定するために、構造ファイルと「規則」のファイル使用する。ＵＤＥはＨＴＴＰトラフィックまたはその他のプロトコルを通過させることができる。ＵＤＥは、ＨＴＴＰトラフィックが到着すると、１）ヘッダ内の「クッキー」の存在、２）指定されたＵＲＬ経路、３）宛先ポート、４）パケットのＳＬ、についてパケットを調べることができる。ＵＤＥは、この情報と規則データベースに基づいて、新規のＳＬと、新規のポート番号とネットワークアドレスをそのパケット用に選択することができる。ＵＤＥの複数のコピーを1つのシステム上で実行することができる。ＵＤＥは、これを流れるトラフィックのＳＬを変更できなければならないという特権を持っている。

【００６７】

さらに、ＴＣＢ２１８（信用計算ベース）機構というセキュリティ機構が信用サーバによって提供される。信用サーバは、「マルチユーザ」または「単一ユーザ」モードであるという既存の概念をとり、これをＯＳ自体に拡張している。標準のＵＮＩＸシステム上では、これらのモードの違いは、単にどのサービス（システムプロセス）が実行されているかということである。モード間の切り替えは、単純にプロセスを停止または開始することで行う。信用サーバシステム上で、標準のプライマリシステムプロセス（“ｉｎｉｔ”と呼ぶ）は、システムが実行（安全）モードまたはメンテナンス（安全性の低い）モードのいずれかにあることを表示するために、内部ＯＳフラグ２１８を変更するべく修正されている。オブジェクトを「ＴＣＢオブジェクト」であると考慮するために、各ファイルシステムオブジェクトのｉノードにフラグがさらに追加される。「ＴＣＢオブジェクト」であるとは、システムが実行モードにある場合、読み出しのためにこのオブジェクトを修正または開くことができないということである。

【００６８】

さらに、信用サーバシステムにより、システムモードによって、様々なセキュリティ機構（ＳＬ機構など）をオンまたはオフにすることができる。そのため、

システム管理者は、各モードにおいてどのセキュリティが有効であるかを定義するために選択を行うことができる。

【００６９】

本発明の信用サーバは、ＵＮＩＸオペレーティングシステムに関連して説明される。その他のオペレーティングシステムでも、本発明のセキュリティ形態を利用して、ワークステーション、メインフレーム、パーソナルコンピュータ、計算可能な装置、無線通信装置のようなあらゆるタイプの計算装置に安全なオペレーションモードを提供することができる。本発明のオペレーションシステムは、システムが管理モードまたは安全オペレーションモードのいずれかにおいて実行され、ファイル記憶構造と実行されるプロセスがコンピュータシステム上の内容を管理する安全性の高い方法を許容するべく修正されるＵＮＩＸオペレーティングシステムに基づいた基礎を有することが好ましい。

【００７０】

データオブジェクトという用語は、プロセスが実行されるあらゆる内容を総称的に表すために使用され、また、これをプロセスに追加的に適用し、実行するイベントのパラメータが、そのプロセス段階の実行以前にチェックされるようにすることもできる。このシステムは、実行する各イベントが、上述したコンポーネント（ＡＳＮ、ＵＤＥ、セキュリティゲート）の各々を備えた、あるいは、これらのコンポーネントの各々が、協働する形で個別に実行される1つの中央イベント制御装置によって扱われる状況で実現することができる。本発明の信用オペレーティングシステムは、ＳＬをサポートし、ユーザまたはプロセスが特定のオブジェクトまたはリソースにアクセスできるかどうかを決定するためにこれらを使用する。ユーザまたは特権を持たないプロセスがＳＬの修正を行うことはできないため、ユーザの服従に頼ることなく、システムのセキュリティポリシーが実施される。システム施行ラベルを用いたこのアクセス制御は、命令アクセス制御（ＭＡＣ）と呼ばれる。

【００７１】

本発明のオペレーティングシステムの安全を保つべく実現される別の規制は、ルートアカウントが、システム管理に関連した全てのプロセスを実行するべく許

可されないスーパーユーザ（ルート）特権のセグメンテーションを必要とする。代わりに、この特権が多数の小型の特権に分割される。そのため、バックアッププログラムがあらゆるファイルを読み出すことができるが、この特権を、システムのシャットダウン、ファイルの修正、ランダムネットワークパケットの送信に使用することはできない。1つの強力な機構の代わりに多数の制限付き機能を使用することは、従来技術では最下位特権の原則と呼ばれている。

【００７２】

本発明の信用オペレーティングシステム上では、ユーザではなくプログラムに特権が与えられる。バックアッププログラムには、ジョブを実行するのに必要な特権のみが与えられ、これによって開始されるプログラムはバックアッププログラムの特権を引き継ぐことはできない。特定のユーザは、ある特定のプログラムを実行する権利を有することができるが、そのユーザのセッションは何らの特権も持たない。特権を備えたプログラムはほとんどなく、その能力は限られ、注意深く制御される。最下位特権を使用することで、標準オペレーティングシステムで共通に報告されているほとんどのセキュリティ問題を排除することができる。特定のスーパーユーザバグが修正されなくても、バグを使用するこの信用オペレーティングシステム上では、悪質なユーザが全てのシステムセキュリティをバイパスすることは許可されない。

【００７３】

この信用オペレーティングシステム上では、ラベリングとＭＡＣが、ファイルおよびプロセスレベルに加えて、ネットワークインタフェースレベルで適用される。例えば、ウェブブラウザのようなアプリケーションは、一般に、プログラムが応答し、インターネットネットワーク接続を介して送信される情報を生成するそのアプリケーションプログラムに定められたデータを識別するために、特定のネットワークインタフェースを聴取するように構成される。本発明では、信用サーバは、アプリケーションをマシンのネットワークと直接接続させず、その代わりに、ＵＤＥがネットワークアダプタと相互動作し、アプリケーションのネットワークサービスのフロントエンドとして機能するべく直接インタフェースする。この方法では、好ましい宛先経路、またはネットワークサービスコンポーネント

に通信をルーティングする前に、ラベル、特権、認可が決定および適用される。例えば、インターネットから入力されるパケットについては、段階３１０で、段階３００（図５）で要求されたホストＩＤ、段階３０４で要求されたプロトコル、段階３０６で要求されたポート番号に基づいてラベルが決定される。受信した組み合わせ用の通信セキュリティレベルがない場合には、ネットワークに、プロトコルの一致（段階３１４）とポートレンジ（段階３１６）が存在するかどうかを決定するためにチェックが実行される。段階３１６に一致が見つかると、段階３２２において、関連するセキュリティラベルがパケットに適用される。次に、事前に付加されたラベルに基づいて、ＵＤＥの前にこのパケットが送信され、このパケットが、聴取者が聴取するべく構成された関連の出力宛先へ送信される。この時点で、このラベルを、より広範囲な規則のセットに従ってパケットを転送するように、ＵＤＥにより修正してもよい。

【００７４】

図８は、出力パケットをドロップするため、また、システムがホスト（段階４００）、プロトコル（段階４０２）、ポートレンジ（段階４０４）、ＳＬ（段階４１０）、ネットワークインタフェース（段階４１４）を認識している場合にはパケットの送信を許可するために、同様の確認段階を使用する出力パケットの処理段階を示す図である。出力パケットは、これを作成したプロセスまたはデーモンのラベルを有する。パケットのＳＬがインタフェースと遠隔ホストの両方に有効でない場合には、入力あるいは出力パケットがドロップされる。さらに、ＳＬをパケットヘッダ内に挿入して、信用オペレーティングシステムがネットワークにかけてセキュリティ情報を共用できるようにすることも可能である。

【００７５】

次に図６を参照すると、受信する通信のタイプに基づいて、ＵＲＬがインターネットベースの通信を要求し、ＬＡＮまたはＷＡＮネットワーク要求が処理される段階３５０においてＵＤＥモードが決定される。既知のユーザに、そのユーザの前回のアクセス中に記憶された情報を指定するクッキーが、段階３７０において利用可能である場合には、段階３７４でクッキーの有効性がチェックされる。クッキーが有効である場合、段階３９０で、ユーザ要求を適切な宛先アドレスに

と、アプリケーションの聴取者が聴取するように構成されたポートに送信するために、センシティビティラベルが、データベースに記憶されたデータに従って変更される。クッキーがない、または無効であった場合には、選択された供給宛先とセンシティビティラベルＳＬがこの時点で決定され、また、クッキーが適切であった場合には、要求が段階３９０へ送信される。さらに適切でない場合には、適した宛先がアレンジできている場合には、要求を別の場所へ送信するために、段階３８６でＵＲＬがセンシティビティラベルとの組み合わせにおいて使用され、そうでない場合には接続がドロップされる。ＵＲＬを使用しない通信は、段階３５４で、ＳＬと共に要求された宛先と事前に定義した適切な組み合わせのテーブルとを比較して扱われ、適切な組み合わせが見つからない場合には段階３５６においてドロップされる。要求がＳＬと正しく一致すると、次に、段階３６０において、ＳＬが、表示された改訂ラベルとポートアドレスに変更され、ここで、データがアプリケーションを聴取できるようになる。

【００７６】

図７は、ＵＤＥが、最初に付加されたラベルに基づいて、要求を別タイプのデータに送信するために使用する構造ファイルの１例を示す。このファイルは、通信が受信され、ユーザのコンピュータに記憶されたクッキーの内容に従って要求を転送する、ポートへのリファレンスを含んでいる。

【００７７】

上述したセキュリティゲート８（図1を参照）プログラムは、２つのプロセス間、またはプロセスとネットワークインタフェース間の通信を制限する特別のプログラムである。その構造ファイルは、あて先ＳＬとポートと共に、ソースＳＬとポートを指定する。例えば、ウェブサーバ５００で処理され、安全なパーティション内にある別の情報へのアクセスが必要な要求が、セキュリティゲート５０４（図９を参照）によって処理され、ここでは、オリジナルのＳＬにある要求５０２が、より高いＳＬレベルで動作しているセキュリティゲート５０４によって受信される。許可された要求は、バックエンド・データベースサーバ５１０の認可されたＳＬと一致するように、そのＳＬをＳＬ１からＳＬ２へ修正されていてもよい。上述したように、ＳＬはディスジョイントであり、つまり、両者はいか

なる形でも相互作用することができない。そのため、セキュリティゲート５０４プログラムに、両者よりも大きなＳＬレンジが与えられる。さらに、両エンドポイントを含むＳＬレンジが、ＳＬセキュリティチェックを無視するが、そのレンジ内のＳＬに限定される特権と共に与えられる。この方法で、要求に反応してデータを生成するために、システムの異なるパーティションまたはコンピュータからのデータが要求に従って結合される。ユーザへと戻る経路上で、セキュリティゲートは、応答を要求側のウェブサーバ５００へ戻すために必要なラベル翻訳を実行する。

【００７８】

ＵＮＩＸオペレーティングシステム用のこのシステムの１例では、修正されたＩｎｉｔカーネルの代わりに、プログラム、ネットワークリソース、実行可能なプロセスに関連したファイル属性が、改訂したロールベースの認可手順と動作するべく修正された標準オペレーティングシステムを使用している。従って、本発明が提供する機能は、各プロセスがユーザのロールと比較される場合に通信を処理するプロセスの確認と、プロセスに許可された特権を拡張するものである。

【００７９】

図１０は、異なるコンパートメントまたはパーティションへのアクセスを許可する、適用される様々な類別に関連したラベルを表示した、単純なセンシティビティラベルのテーブルのサンプルである。例えば、セキュリティゲートがこのテーブルを使用して、要求を、別のコンピュータや、同じコンピュータの別のパーティション内に位置するために直接アクセスできないデータへと送信されるようにすることができる。

【００８０】

図１１（バイナリフロー）を参照すると、プロセスがファイルを実行する場合、信用サーバが、実行前にプロセスとファイルの両方に質問をする。プロセスとファイルのセキュリティ属性は、図４に示すように既に確立されている。（図４中の２００は、図１１中の６００と関連している。）

【００８１】

段階６００で許可ビットがチェックされ、次に、プロセスＳＬ（２７２）がフ

ァイルＳＬ（２９２）と等しい、またはこれよりも大きいことを確定するために、段階６０４でＳＬラベルが確認される。

【００８２】

段階６０８で、アクセス認可セット（２８０）に挙げられたアクセスの少なくとも１つを有するかどうかを決定するために、データベース内でプロセスユーザＩＤ（ＵＩＤ）（２６２、図示せず）が調べられる。

【００８３】

これまでの確認段階のいずれかが失敗していると、バイナリプログラムを実行する許可が拒否される。

【００８４】

段階６１２で、信用サーバが、プロセスＵＩＤ（２６２）に関連した認可を特権認可セット（２８２）と比較する。プロセスＵＩＤ（２６２）が特権認可セット（２８２）に挙げられた認可の１つまたはそれ以上を有する場合には、段階６２０で、信用システムが、ファイルの固有特権（２８６）と認可された特権に記載された特権を持ったバイナリを実行する。プロセスＵＩＤ（２６２）が、特権認可セット（２８２）に記載された認可のどれも持たない場合には、段階６１６で、信用セットが、ファイルの固有特権（２８６）に記載されているが、特権認可セット（２８２）には記載されていない特権を持ったバイナリを実行する。

【００８５】

認可データベース内のＵＩＤ認可とファイルの特権セットの組み合わせは、プロセスＡがファイルを実行する際に得られるプロセスＢを与えられる特権を決定する。例えば、特定のプロセスＵＩＤ（２６２）に、認可データベース内のＭＡＫＥＩＤＢ認可が与えられてもよい。（ＭＡＫＥＩＤＢ（２８０）値は、特定の動作を実行するための認可を持ったプロセスを許可する、定義されたロールを参照することができる。）プロセスＵＩＤ（２６２）がＭＡＫＥＩＤＢ認可（２８０）を持っている場合には、プロセスが図４のファイルを実行した際に、ファイルが実行する。プロセスＵＩＤがＤＥＢＵＧもＭＡＫＥＩＤＢも持っていない場合には、そのプロセスは図４のファイルを実行することができない。

【００８６】

さらなる例として、プロセスのＵＩＤがＡＵＤＩＴＳＹＳ認可を持つ場合には、そのプロセスがテーブル４のファイルを実行した際に、結果として得られるプロセスに、ファイルの認可された特権（２８４）、この場合はＰＶ＿ＰＶ＿ＦＩＬＥが付与される。（ＰＶ＿ＰＶ＿ＦＩＬＥは、プロセスにファイルの特権を変更させる。）そのため、ＡＵＤＩＴＳＩＳ認可を備えたＵＩＤを持つプロセスが図４中のファイルを実行すると、その結果のプロセスは、ファイルの特権を変更する特権を有することになる。しかし、ＵＩＤがＡＵＤＩＴＳＩＳもＢＯＯＴ認可も持っていないプロセスが図４中のファイルを実行する場合には、その結果のプロセスは、ファイルの特権を変更する特権を有さない。これらの例は、このシステムによって提供された機能をデモンストレーションするために使用され、この方法論の潜在的使用を抑制することを意図するものではない。

【００８７】

本システムは、特権を持たないホストまたはインタフェースから入ってくるトラフィック用の「デフォルトウェブサイト」７を備えている（図１）。悪質なユーザがウェブサイトを破壊または改悪することを阻止するために、ウェブページを読み出し専用パーティション内に個別に記憶することができる。これにより、悪質なユーザが、ＣＧＩスクリプトのような、商用ウェブサーバまたはウェブアプリケーション内のホールを使用して、サイトのウェブページにダメージを与えることを不可能にする。エクストラネットのウェブサーバでは、ＵＤＥ４とデフォルトウェブサーバ７を別々のハードウェアプラットフォーム上に設け、安全ネットワークサービスを用いてこれらを接続することができる。

【００８８】

信用サーバシステムの認証モジュール９を、アクセスを許可する前に、ユーザにユーザＩＤの提示と、サイトが定義可能な認証応答（例えば、パスワード、バイオメトリックデバイス、スマートカード、またはアクセストークンチェック）を要求するように構成することができる。ユーザが認証されると、ＵＤＥにより、後続のウェブ要求が認証されたセッションの１部として識別され、別の規制されたパーティションとの通信が許可される。

【００８９】

ここで、図１６のアーキテクチャにおけるデータの流れを、エクストラネット環境、バックエンド/レガシー・アプリケーションサポート、認証コンポーネントの使用の３つの例を用いて説明する。

【００９０】

次に図１３を参照すると、本発明は、互いに隔絶された２つまたはそれ以上のセンシティブウェブサイトをホストするエクストラネットサーバとして構成することができる。エクストラネットウェブサーバの仮想分離により、管理者はシステムを、同一のＵＲＬを用いてアクセスするユーザが、異なるウェブページを得られるように構成することができるようになる。

【００９１】

この構造の１例は、従業員、顧客、株主、その他の人達がアクセスできる企業ウェブサーバである。情報のセンシティビティは各カテゴリによって異なるため、データ保護が重要な問題となる。この場合、システム上で実行されている３つのウェブサーバ（エクストラネットＡ、エクストラネットＢ，エクストラネットＣ）に安全なエクストラネット機能を提供するために、セキュアサーバが使用される。関連するコンポーネントは、ＳＫＩＰを介したＶＰＮ２０、アップグレード/ダウングレードエンフォーサ４、信用サーバ２２である。

【００９２】

段階１００で要求がシステムに入力されると、この要求はまず、段階１１０で暗号化モジュール（ＶＰＮ）２０を通過する。暗号化モジュール２０は、段階１１２において、要求のＩＰアドレスを認証する。次に、段階１３０において、ＩＰアドレスに基づいてこの要求にセンシティビティラベルが指定されるか、または、要求のＩＰアドレスが、段階１２０でＡＳＮによって認識された特別なアドレスでない場合には（つまり、そのＩＰアドレスへのエントリがホストレンジテーブル内にない場合には）、デフォルトラベルが使用される。最終的な宛先を決定するためにポートが使用され、また、図５を参照して既に説明したように、ＳＬが指定される。

【００９３】

次に、段階１４０にて、要求がアップグレード/ダウングレードエンフォーサ

（ＵＤＥ）４へ送られる。ＵＤＥ４は、その要求のセンシティビティラベルを検索し、ラベル付けされたパケットを関連するウェブサーバへ送る。例えば、入力された要求にセンシティビティラベル“ＥｘｔｒａｎｅｔＡ”が指定されている場合、段階１４２で、ＵＤＥ４がこの要求をエクストラネットＡウェブサーバ２４へ転送する。エクストラネットＡウェブサーバ２４は、“ＥｘｔｒａｎｅｔＡ”とラベル付けされた接続のみを受け入れる。図６は、実際に実行される段階をより詳細に示したものである。これ以外の要求は全て拒否され、インターネットからこのウェブサーバへの直接接続が阻止される。

【００９４】

別の例は、ＥｘｔｒａｎｅｔＡ２４とＥｘｔｒａｎｅｔＢ２６の２つのエクストラネット環境にアクセスできるＩＰアドレスからの要求である。まず、段階１１０で、ＩＰアドレスが確認され、ネットワークパケットが暗号化される。次に、ＡＳＮモジュールが、この要求に“ＥｘｔｒａｎｅｔＡ、ＥｘｔｒａｎｅｔＢ”のセンシティビティラベルを指定する。段階１１２でＩＰアドレスが確認され、段階１３０でＳＬが指定された後、段階１４０にて、要求がアップグレード/ダウングレードエンフォーサ（ＵＤＥ）へ送られる。ＵＤＥ４はこのＵＲＬ要求をパースし、どのウェブサーバがこれを受け入れるべきかを決定する。次に、ＵＤＥ４は、要求のＳＬを、宛先ウェブサーバのＳＬと一致するように変更し、次に、許可、アクセス、認可がこの変更を許可すると、要求を適切なウェブサーバへ送信する（段階１４２または１４４にて）。

【００９５】

このアプローチは、エクストラネットサーバに直接接続しようとするあらゆる試みを無効にし、アクセスはＵＤＥ４を介してのみ認められる。サーバは隔離された環境で動作しているため、エクストラネットサーバソフトウェア内のバグを利用しようとする試みがそのサーバ上の他のアプリケーションに悪影響を与えることはない。

【００９６】

セキュリティゲートを用いて、このシステムを、ウェブインタフェースとバックエンド・アプリケーション間に安全な接続性を提供するように構成することが

できる。ウェブサーバは、バックエンド・アプリケーションからのグラフィック形式での情報を表示することのみを目的として機能し、公共または企業ネットワークによってアクセス可能である。例えば、ある銀行が、全ての顧客にインターネットバンキング機能を利用してもらいたいと希望したとする。顧客の中に悪質な人物がいるかもしれないという危機から、ウェブサーバとバックエンド・アプリケーションを別々の仮想環境内に分離することで、センシティブデータを保護する必要がある。このシステムは、これらにアドレス指定をするための安全な方法を提供する。セキュリティゲート８コンポーネントを用いれば、ウェブサーバとバックエンド・アプリケーション間に直接データが流れることはない。全ての要求はセキュリティゲートを通過し、ここで、要求され、システムによって許可されたデータにアクセスする必要がある際に、要求のセンシティビティラベルがバックエンド・アプリケーションのレベルに上げられる。

【００９７】

図１４は、統計的なウェブページを表示するため、また、バックエンド・アプリケーションへの接続性を提供するために使用されるウェブサーバを示している。段階１６０にて、情報はセキュリティゲートを通過する。バックエンド・アプリケーション内のデータが独自のコンパートメント内に常駐し（独特のセンシティビティラベルを有する）、バックエンド・アプリケーションがセキュリティゲート８を介してしかアクセスできないようにする。このアプローチを用いることにより、インターネットインタフェースから内部インタフェースへ、またはその逆において、情報を直接送信しようとするあらゆる試みが無効とされる。

【００９８】

特定のユーザが使用するＩＰアドレスをサーバが常に予想することは不可能である。例えば、再び図１６の頂部を参照すると、ユーザは、ダイナミックＩＰアドレス指定を使用しているサービスプロバイダ（ＩＳＰ）と接続することができる。また、ユーザは、公共の「情報キオスク」から、またはどこか他の場所にあるマシンから接続することも可能である。このような場合には、ユーザに、規制されたウェブサーバまたはアプリケーションへのアクセスを許可できることが重要である。認証モジュールは、ユーザをシステムへ認証させ、後続するユーザの

セッション内にある全ての要求を適切な規制されたサービスへと送信する。段階１１２でＩＰレベルの認証を使用できない場所から接続しているユーザは、段階１２０でデフォルトウェブサーバへ送られる。デフォルトウェブサイトによって、段階１２２での認証モジュールへのアクセスが可能になる。認証モジュールは、個別のコンパートメント内で実行されている保護されたアプリケーションであり、セキュリティゲートを介してのみアクセスすることができる。

【００９９】

好ましい実施例では、認証モジュールの相互作用は、全てのセッショントラフィックを暗号化するためのＳＳＬを使って保護されている。ユーザが認証されると、段階１２４で認証モジュールが秘密のマーカ（クッキー）を提供する。次に、この秘密のマーカはが、本システムとの通信におけるユーザのブラウザによって挿入される。さらに、認証モジュールは、段階１２８において、マーカのＵＤＥと、関連するセンシティビティラベルに通知を行う。ユーザが認証されると、ＵＤＥがユーザの入力要求を、適切な規制されたウェブサーバへ転送する。ＵＤＥはマーカ上のタイムアウトを施行する。ＵＤＥが、タイムアウト時間よりも長い時間においてマーカを見つけられなかった場合には、マーカは無効となる。接続を復元するには、ユーザは、段階１２２で再び認証モジュールを使用しなければならない。

【０１００】

図１５は、最初にデフォルトウェブサーバを介して認証モジュールへと流れ、その後、ＵＤＥによって規制されたエクストラネットへ転送されるトラフィックを示す。

【０１０１】

ネットワークを区分する機能は、クリティカルなネットワークおよびトランザクションサーバをサポートするのに必要なレベルの確実性を提供する上での、本発明の信用オペレーティングシステムのキーコンポーネントである。次に図１２を参照すると、同一のセンシティビティラベルを有するプロセス、ファイル、その他のリソースは、同一のコンパートメントまたはパーティション１１内に存在すると思われる。プログラム、データ、ネットアークインタフェースを、パーテ

ィション間のアクセスが規制された、別々の隔離されたパーティションに分けることができる。例えば、特定の機能に関連したバックエンド・アプリケーションを、相互に、また、一般人がアクセスできる、外的アクセス可能なコンパートメント１１から隔離された別々のアプリケーションコンパートメント１２、１３に記憶することができる。あるコンパートメントに関連したパケットは、別のパケット内のアプリケーションまたはネットワークサービスが読み出しや妨害を行うことはできない。システムが、異なる部門からのユーザや、別のインタフェースやホストと相互作用するネットワークデーモンのような異なるクラスのユーザおよびジョブを扱う場合、区分は重要なセキュリティ機能である。

【０１０２】

ユーザが信用サーバに接続する際、または、信用サーバを介してデータを要求する際に、そのユーザが現在実行されているロールまたはセンシティビティレベルと同格での実行を許可されたということで、プロセッサがユーザをプロセスのテーブルと関連付ける。プロセスによっては、ユーザが公共のインターネットウェブページにアクセスする時のように、アノニマスで実行できるものもある。信用サーバはアノニマスなユーザをパーティションへ誘導し、ここで、ユーザ要求に低レベルセンシティビティラベルが指定される。個別のパーティションが、実行またはビューが可能である使用可能なプロセスまたはファイルを独占的に規制する。プロセスはセキュリティ機構によってバインドされ、ここで、ｈｔｔｐのようなサービスが、コンピュータの構造の限られた部分へのアクセスを許可する。

【０１０３】

プロセステーブルは、ユーザを個々に、またはロールにおいて記述することができる、そのプロセスに関連した１組のユーザ認可特権を追加的に有することができる。制御されたリソースへアクセスを許可する前、また、要求されたプロセスを実行する前に、この第２の特権と認可情報をチェックするためにカーネルが採用される。

【０１０４】

好ましい実施例では、プロセステーブルは、信用サーバに記憶されている、暗

号化された読み出し専用データ構造のファイルである。このテーブルの管理と制御は、システムのメンテナンスモードにおいてアクセスされることが好ましい。管理機能は、許可されたユーザが、管理モードにある際にメンテナンスモードを実行できるように、信用サーバの記憶装置内の個別のパーティションに記憶される。

【０１０５】

認可は、信用オペレーティングシステムにおけるユーザアカウントの属性であり、ユーザにオペレーティングシステムアプリケーションおよびユーティリティのサブセットの実行を可能にさせるものである。特権は、アプリケーションに指定された属性であり、アプリケーションに、プロセスまたはリソースへの異なる等級のアクセスを提供する。この２組の属性を一緒に使用することで、プログラムが、使用するユーザによって動作を変更することができるようになる。アプリケーションを、ユーザに許可を与えるためにアプリケーションとオペレーションプラットフォームを通信させる標準化されたプロトコルを提供することで、新規の認可を定義およびチェックするべく拡張することもできる。さらに、管理デューティを、後に異なるユーザに指定される別々のロールに分割するために認可を使用することもできる。

【０１０６】

システムのユーザは、特定のロールからプロセスを実行することができ、次に、このプロセスが、最初のユーザまたはシステム要求から許可されると、プロセッサにより送信または受信された最初の要求を追跡するプロセスに、認可のセンシティビティレベルを指定する。Ｏ/Ｓのカーネルは、特定のロールのセッション中にはユーザに最新のユーザＩＤ情報を変更させない。この方法では、要求されたタスクを実行するのに必要なロールまたは特権レベルが、要求を受信する最下位プロセスのみが、次の、要求またはプロセスにサポートされた最高レベルのプロセスへの通過を許可されるように制限される。例えば、データベースアプリケーションから印刷要求を開始するユーザが、まず、データベースの、ユーザのロールに基づいてビューを許可される部分のみへのアクセスを許可される。データベーステーブルの各行は、その記録を見るために必要な認可レベルまたはロー

ルを反映する拡張された属性を有することができる。これは、その行へのデフォルト許可が、その行を挿入したユーザのレベルに関連する行挿入ポイントにおいて定義される。この方法では、検索される記録のレベルを決定するために、このレポートがユーザのロールを決定する。次に、印刷プロセスはデータベース中のそのロールのレベルに関連した行だけを印刷させられる。続いて印刷プロセスは初期化され、その後、送信者のレベル、検索したデータのレベル、またはユーザが選択したプリンタデバイスのレベルで実行される。例えば、ユーザが、離れた場所にあるために、プリンタへのルート上の内容を適切なレベルの安全性で保護することができないプリンタを選択した場合、プリンタと選択されたルートがサポートすることができるレベルのデータのみが最終的にプリンタへ送信される。生成または実行された任意のコマンドは、最下レベルのプロセスのロールしか受信しないため、印刷プロセスは、データストリームに隠されているかもしれない、組み込まれた高レベルのプロセスコマンドを実行するその他のトランザクションを実行することは許されない。賢いユーザまたはハッカーが別のプロセス段階にコマンドを組み込めたとしても、システムは、指定されたプロセスレベルを超えるトランザクションを許可しない。これは、システムの主な管理機能は、システムの記憶装置パーティションから、セキュアモードで実行または使用することができないためである。従って、プリンタ処理段階は、推測されるロール内で、このロール以外のプロセスを開始しないように指示される。

【０１０７】

インターネットベースのウェブユーザがファイアウォールの後ろにあるリソースへのアクセスを要求する例では、システムはまず、元来指定されているレベルから、要求の誘導方法と、開始するために許可するべきプロセスを決定する。ユーザのレベルが認可されたものでない場合には、要求した情報は利用できない旨のメッセージがユーザに提示される。ユーザは、要求されたデータが見つからないか、または、ユーザは追加のセキュリティアクセスプロセスを使って再度ログインすることができるというメッセージを受け取る。

【０１０８】

ネットワーク層暗号化は、このアーキテクチャのオプションコンポーネントで

ある。ＨＴＴＰセッショントラフィックのみを暗号化するためにＳＳＬ（Ｎｅｔｓｃａｐｅ、Ｍｉｃｒｏｓｏｆｔその他によりサポートされている）を使用するため、ネットワーク層暗号化コンポーネントの主な目的はＩＰアドレスを認証することである。特定の機能（例えば、管理ツールや、規制されたエクストラネットウェブサーバ）へのアクセスを、ユーザがどのホストから来ているかに基づいて許可する場合には、ホスト認証が重要となる。このシステムではあらゆるネットワーク層暗号化モジュール（ＶＰＮ）を使用することができるが、構造図ではＳｕｎ　ＭｉｃｒｏｓｙｓｔｅｍのＳＫＩＰを使用している。

【０１０９】

ＳＳＬプロキシ３（図1を参照）も、やはり本発明のオプションコンポーネントである。ＳＳＬは、セッション層の暗号化を提供する。あらゆる特定のユーザセッションは、ウェブアプリケーションがどのように書かれ、構成されているかによって、ＳＳＬと非暗号化ｈｔｔｐトラフィック間の切り替えを行うことができる。例えば、ユーザは、デフォルトのウェブサーバからＨＴＭＬページを検索する際に非暗号化チャネルを使用することができるが、ＳＳＬは、センシティブまたはプライベートな情報や要求を扱うアプリケーションによって使用可能にされる。ＳＳＬプロキシは、サーティフィケート、クッキーのような全ての要求情報を保存する。この後のモジュール、例えばアップグレード/ダウングレードエンフォーサ（ＵＤＥ）４やその他のウェブサーバがこの情報使用することができる。このシステムは一般的なＳＳＬプロキシを使用しており、市販されているこれ以外のＳＳＬ製品で代用することもできる。

【０１１０】

パーティションに基づいた制御アクセス方法に加えて、特定のセンシティビティレベルでシステムにアクセスするユーザが、オブジェクトを要求することで、異なるプロセスまたはデータファイルに誘導されるようにするために、プロセス関係を定義するべくテーブルが提供される。この方式では、ソフトウェアアプリケーションスイートに制御方法を付加することができ、これにより、ユーザは自分のセンシティビティレベルにおいてオペレーションを行ったり、データを見ることが許可される。これによって、例えば、階層セキュリティシステムがソフト

ウェアアプリケーションスイートに外部的に付加されるように市販のソフトウェア製品を実行することができ、ここで、ソフトウェアを実行する各ユーザには、カストマイズまたはパーソナライズされたバージョンが供給される。あるユーザは１組の特権で接続することができ、またあるユーザは同じアプリケーションを別の特権で実行することができる。例えば、各個人は、そのアイデンティティとロールに基づいて、通常の許可ビットを持ったプログラム上にアクセシビリティ規制を定義または配置することなく、リソースまたはコンテンツへの異なるアクセスレベルを許可するべく、本発明のサーバ上に保存されているワードプロセッサアプリケーションを使用することができる。これにより、システムは、ユーザが使用可能なコンテンツをダイナミックに修正できるようになるが、この機能は、一般にはワードプロセシングプログラムの許可を介してユーザに提供されることはない。これによりこのシステムは、各アプリケーションソフトウェアプログラムに特定のプロプリエタリー制御方法を用いて各アプリケーションを別々に構成する代わりに、１組のセキュリティ制御アクセスをシステム上の全てのアプリケーションに適用できるようになる。このタイプの構造をオペレーティングシステムレベルで確立することで、システム管理者は、各々のアプリケーションの認可機構を全て知る必要がなくなり、代わりに、本発明のグローバル制御によってデータまたはプロセスを保護することができるようになる。この方法では、属性および認可のワンタイムアプリケーションが、ソフトウェアの実行方法を形式的に決定することができる。同様の方法で、アプリケーションプログラムのアーキテクチャ内のプロセスを認可する代わりに、このワンタイム属性定義を実行することで、オペレーティングシステムにおいて、実行される実際のプロセスコールを規制的に個別に制御することができる。好ましい実施例では、システムレベルを、認可の部門ごとの管理レベルに従って分類または定義することができる。別の実施例では、プロジェクトマイルストーン、タイムライン、伝送イベント、またはその他のシステムイベントに関連してアクセシビリティを変更するために、スケジュールを採用することができるワークフロー式の方法論に従ってレベルを生成および適用することができる。例えば、特定のプロセス実行段階へのアクセスやデータアクセス機能を選択的にロックまたはフリーズするためにプロセス段

階を確立することができる。このプロセス段階では、ユーザは、プロセス内のある時点において完全な特権を有することができるが、その後、この特権が全くなくなるか、データまたはプロセスの実行上の読み出し専用機能だけを備える。

【０１１１】

ユーザがアプリケーションを実行することによりデータ要求をトップシークレットコンピュータシステムに転送する信用サーバ上でプロセスを実行した後にのみ、トップシークレットコンピュータへのアクセスが許可されるコンピュータシステムに、信用サーバ２２によって提供された制御を適用することもできる。このタイプの制御は、他のネットワークデバイスへのアクセスや、プロセスが他のパーティションと制御された方法で通信するマシンのパーティションへのアクセスを提供するためにも使用される。

【０１１２】

例えば、ＨＴＴＰデーモンや関連するＣＧＩスクリプトのようなネットワークサービスに、ファイル（例えば、クリティカルなウェブページやＣＧＩディレクトリ）への読み出し専用アクセスを付与することができ、また、これらのネットワークサービスを他のリソース（例えば、内部ネットワークインタフェース、システムファイル、他のネットワークデーモン）から完全に隔離することができる。この方法で構成されたネットワークサーバは、たとえ、市販のソフトウェア内に、アクセスしたユーザがマシンインストラクションのあらゆるランダムシーケンスを実行できるようにしてしまう有害なバグが存在している場合でさえも、そのウェブページとＣＧＩスクリプトを外部接続からの修正から保護することができる。ネットワークサービスから別のネットワークインタフェースおよびホストへのアクセスも、容易に制限することができる。

【０１１３】

本発明により、複数のウェブサーバを、それぞれ隔離したパーティション内で実行することができる。エクストラネットの各サービスへのアクセスは、ＵＤＥ４によって規制される。さらに、本発明の全ての仮想ウェブサイトにあるように、個々のファイルを読み出し専用として保護することができるため、本発明のサーバ上にインストールした市販のウェブサーバソフトウェアスイートに使用可能

なホールが見つかった場合でも、ウェブサイトへの悪質な改悪を阻止することができる。

【０１１４】

読み出し専用ファイルおよびディレクトリは、隔離された複数のウェブサーバによって共用することが可能である。これにより、共通のウェブページおよびアプリケーションのコピーを１つ使えば済むため、ファイルのコピーを省くことができ、管理オーバヘッドを減らすことができる。ＵＤＥとエクストラネットウェブサーバを、同じ１つの物理マシン上に常駐させたり、ＡＳＮソフトウェアのネットワークレベルの暗号化機能とセキュリティ機能を用いて接続した別のシステム上でエクストラネットを実行することが可能である。

【０１１５】

本発明は、ローカルおよび遠隔管理の両方に設けることができる。信用管理ユーティリティへは、アクセスを許可されたアカウントを持つユーザが、認可されたホストから来ている場合のみにアクセス可能である。ＵＤＥは、ＡＳＮモジュールにより付加されたラベルを使用して、入力パケットを信用管理ウェブサーバパーティション６へ送信することができるかどうかを決定する。好ましい実施例では、ＡＳＮモジュールは、イントラネット内のネットワークデバイスへの管理機能を規制する。例えば、ＵＮＩＸベースのシステムにおいて、ユーザ管理、システムシャットダウン、特権およびラベルの修正に関連した管理機能へは、システムの特定の管理者が実行するＩＮＩＴ手順を用いてシステムの内部を初期化した際のみにアクセスすることができる。

【０１１６】

本発明の信用サーバの管理は、コンソールからの直接ログインを介して、またはネットワーク接続を介して行うことができる。ネットワーク接続は、拡張したＳＳＨコンポーネントを用いて、または信用管理ユーティリティを用いて実施される。管理ウェブサーバ、管理ツールおよびユーティリティへのアクセスは、管理パーティションへアクセスできるように構成されている特定のＩＰアドレスと特定のネットワークインタフェースのみに限定される。ＩＰアドレスは、ネットワークレベルの暗号化コンポーネントを使って認証される。

【０１１７】

このシステムはさらに、システム管理を簡単にするためのブラウザベースの管理ツールを提供する。管理者はＵＮＩＸシステム管理や、その他のＵＮＩＸ管理ソフトウェアについて詳細に知る必要はない。ブラウザベースのツールは、特定のタスクにプロセスを構成する上で管理者をアシストする要求に応じて実行されるプロセスのマップをグラフィカルに表示することができる。記述的な情報が提供されるため、管理者は、実行されたプロセスの履歴を見るため、または、プロセスへのセンシティビティレベルの適用をテストするために実行されたプロセスの１部分のために実行されたプロセスを追跡することが可能である。さらに本システムは、システムを実際に区分する前にプロセスがロールによってセグメントされるパーティション定義においても補助を行う。この方法で、実現の前にシステムをテストすることができる。システムおよびパーティションへのアクセスは、ユーザの地理的範囲をサポートするように実現することもできる。システム内にシミュレーションソフトウェアを統合して、所望のプロセススループットを達成するべくあらゆる処理ルーチンを繰り返せるようにすることにより、この時点でパフォーマンスのチューニングを実行してもよい。実際の使用中に、このタイプのグラフィックユーティリティは、ユーザのプロセスインタラクションと要求を表示する上で補助を提供することもできる。この表示では、オリジナルシステム内に定義された所定の経路を逸脱する全てのプロセスについて、出力が、ｅ－メールプロセスを使って管理者へ送信される。最終的に選択され、テストされたグラフィック表示をフリーズして、他のプロセスが許可されないようにしてもよい。本システムのこのグラフィックモデルは、表またはリンクされたリストの形式に修正され、プロセスアクティビティを制御するためにＵＤＥとセキュリティゲート８によって使用される。各プロセスを分析するのと同じ方法で、全体的なシステムレベル分析を実行できる。この場合、全体のプロセスパフォーマンスの制約を決定するために、各プロセスを起源のプロセスストリームにまで追跡することができる。

【０１１８】

全てのタイプのインターネットトランザクションのための、信頼性の高い安全

な基準として、本発明は、全タイプのデータベースゲートウェイシステム用のトップシェルフ・セキュリティソリューションである。例えば、患者の病歴や処方箋の記録を、インターネットを介して地元または遠隔地のユーザに提供したいと希望する医療機関は、患者のプライバシーを考慮しなければならない。このシステムは、インターネットユーザにアクセスを認可すると同時に、プライベートなデータをオペレーティングシステムレベルで攻撃から保護するためのセキュリティフレームワークである。

【０１１９】

このシステムはＵＮＩＸバージョンの標準Ｓｏｌａｒｉｓアプリケーションとの１００％の互換性を持っているため、Ｂｒｏａｄｖｉｓｉｏｎ、Ｎｅｔｓｃａｐｅ、Ｏｒａｃｌｅ、Ｅｒｇｏｎ　Ｉｎｆｏｒｍａｔｉｋ、Ｎｅｔｌｉｆｅ　ＧｍｂＨ、Ｎｅｏｎ、ＢＥＡ、その他を含む、市販されているあらゆる既製のバンキングおよび電子商取引アプリケーションのためのセキュアアプリケーションプラットフォームとして使用することができる。

【０１２０】

バンキングソリューションに加えて、本発明は、これ以外の多数のタイプの金融システム、例えばオンラインの仲買業務や保険オペレーションに非常に適している。ウェブベースのトランザクションを分割するための安全でコンパートメント化されたフレームワークを提供することにより、本発明は、産業および医療の供給チェーン管理システムにとってさらに理想的なソリューションとなる。外部のサプライヤおよび他のユーザによる内部サービスへのアクセスを制限している企業は、１つのシステムを多数の専用仮想システムにトランスペアレントに区分するパーティションを作成する。

【０１２１】

製造業環境では、個々の部品サプライヤが、カスタマイズされたエントリ画面を含んだウェブサイトにアクセスすることができ、同時に、同じシステム上において、マネージャは、ベンダー間の価格比較を容易にするため、また、出荷変数を調整するために、セキュアパーティション内でオーダーフルフィルメント・データベースインタフェースを実行することができる。適切な認可を持っていない

通常のユーザは、その企業や製品およびサービスについて知ることができる企業の公開ウェブサイトへ回される。パケットラベリングにより、１つのパーティションへのアクセスを認可されたユーザは、別のパーティションにおけるサービスへのアクセスを得ることはできない。

【０１２２】

医療環境では、患者の病歴を安全に記憶し、これをインターネットを介して病院のブランチ間で送信できると同時に、別のウェブサービスでは、認可された薬剤師に処方箋情報を送信することができる。認可されていないユーザは、アクセスを完全に拒否され、組織の公共ウェブサーバに運ばれる。ラベリング機構により、処方箋情報パーティションの使用を認可された薬剤師は、患者の病歴パーティション内の情報やプログラムへアクセスすることはできない。

【０１２３】

本発明を、公共のネットワークにかけてアクセス可能または読み出し可能であるが、無認可の外部からの改悪からは完全に保護されたウェブサイトの作成に使用することができる。本発明を使用して、読み出しアクセスは許可されるが、書き込みアクセスは拒否されるパーティション内にウェブページを記憶することができる。これなら、悪質なユーザが既存の情報を変更してウェブページを破壊したり、猥褻な画像をポスティングしたり、ウェブサイトコンテンツを変更したりすることができないので、管理者は安心である。このシステムを採用したウェブサイトは、ウェブサーバアプリケーション内のバグを利用した攻撃からも保護される。

【０１２４】

指定される属性のタイプは、コンピュータ上の利用可能な記憶装置によってのみ、システム内で何らかの値または制御を提供するという範囲内で制限される。システムの管理者は、利用可能なレベルを制限するために、レベルの実用性を採用してもよい。さらに、例えば、ユーザが、特定レベルの認可、またはあるプロジェクトに関連したアクセスを用いてアプリケーションを実行する特権を持ちながら、同時に、第２プロジェクト上ではその同じプロセスを実行する権利を持たないというマトリックスベースのアクセス方法を採用することもできる。これま

で、このタイプの制御は、マルチロールユーザをサポートするようにプログラムされた特定のソフトウェアアプリケーション内でのみ利用可能であった。

【０１２５】

本発明の信用オペレーティングシステムはさらに、ユーザのログインに関連した、拡張されたアカウントセキュリティ機能を採用し、コンピュータがランダムに付与したプロナウンス可能なパスワードのリストを提供し、その中からユーザが１つを選択できるようにした。この機能は、ユーザが共通の言葉や名称をパスワードに使用することを防止する。システムはさらに、最大長さがシステムにより定義可能な（つまり３１文字）長いパスワードをサポートする。信用オペレーティングシステムは、ダイナミックライブラリの置換を介して、デフォルトのパスワード暗号化アルゴリズムを別のアルゴリズムで置換するための機構を提供する。識別および認可ログインプロセスを、追加のシステム専用認可チェックを含むように拡張することができる。この１例に、ログインするために、「特別な特権」アカウントを、追加のアカウント名およびパスワードと共に強行し、セキュリティをさらに強化できるプログラムがある。これ以外の向上した手段、例えば、バイオメトリック識別またはアクセストークンも、この特徴を使って搭載することができる。

【０１２６】

信用オペレーティングシステムは、アプリケーションが、標準のオペレーティングシステムよりも幅広いセキュリティ関連のイベントを追跡することができる、拡張した監査機構を採用している。これらのトランザクションに関する情報が、任意のアクセス制御機構と命令アクセス制御機構の両方によって保護された隔離されたパーティション内の監査トレイルに付加される。このアプローチにより、侵入者がトラックをカバーし、ペネトレーションの痕跡を消すことを防止する。監査記録を保護することで、訴訟や法の執行をサポートするのに十分な証拠が保持される。

【０１２７】

【発明の効果】

内在するオペレーティングシステムＡＰＩとの１００％の互換性を維持するこ

とができ、また、経費と時間のかかる統合作業を大幅に縮小することができる。

【図面の簡単な説明】

【図１】　本発明のシステムの構造の概略図である。

【図２】　システムのファイルのサンプルiノード構造である。

【図３】　信用サーバシステムのプロセスおよびパケットのサンプルiノード構造である。

【図４】　プロセスパケットおよびファイルのサンプルデータを備えたiノード構造の表である。

【図５】　入力されるパケットのフロー図である。

【図６】　本発明のＵＤＥによる処理のフロー図である。

【図７】　ＵＤＥによって使用されるサンプル構造ファイルである。

【図８】　出力されるパケットのフロー図である。

【図９】　セキュリティーガイドの流れを示す図である。

【図１０】　ＳＬとコンパートメントのサンプル表である。

【図１１】　バイナリデータを実行するための処理段階のフロー図である。

【図１２】　本発明の高レベルのブロック図である。

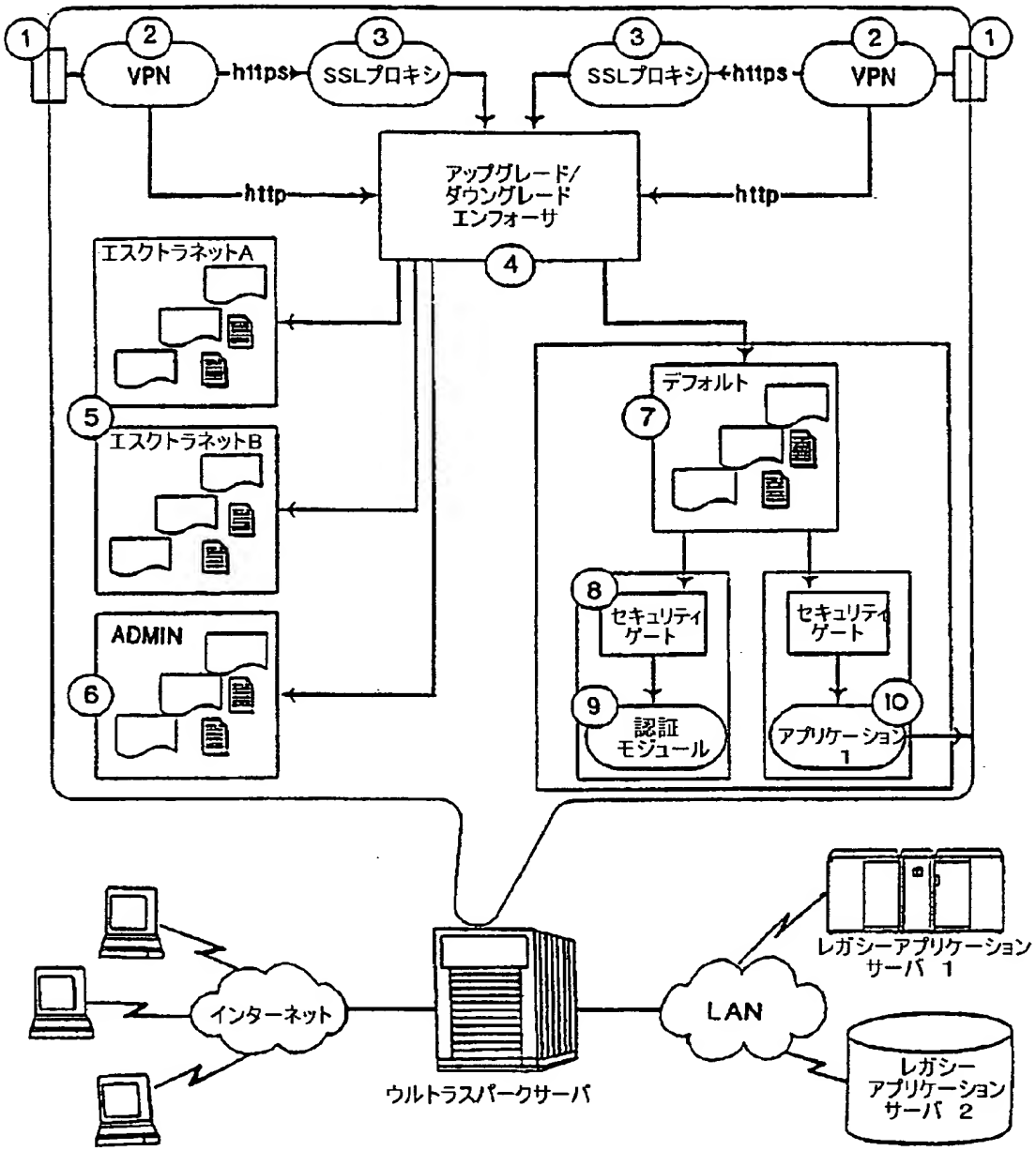
【図１３】　エクストラネットアクセス例における、インタラクトするコンポーネントの図である。

【図１４】　レガシーアプリケーション／バックエンド環境の図である。

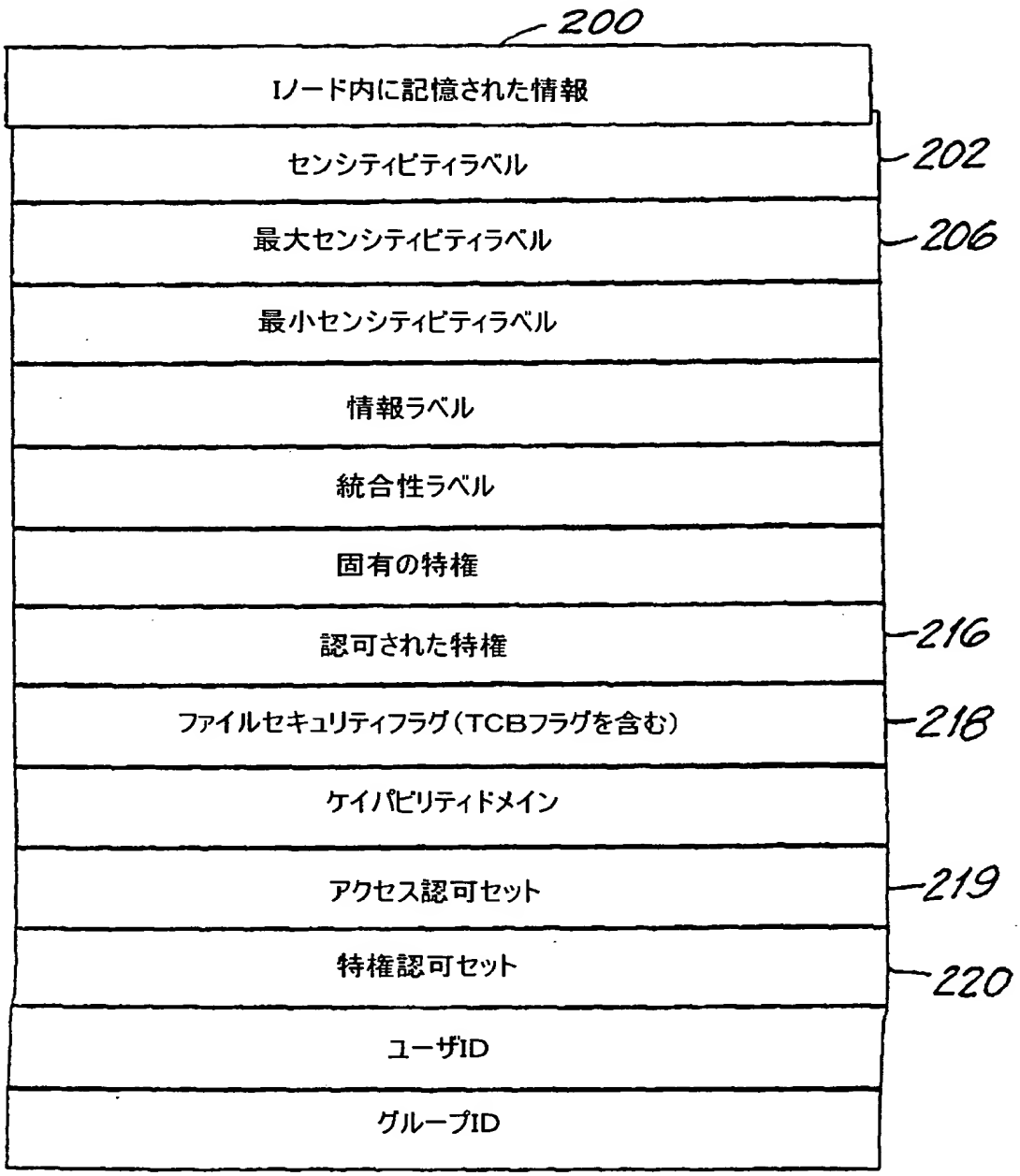
【図１５】　認証モジュールデータのフロー図である。

【図１６】　本発明の処理段階のデータフロー図である。

【図１】

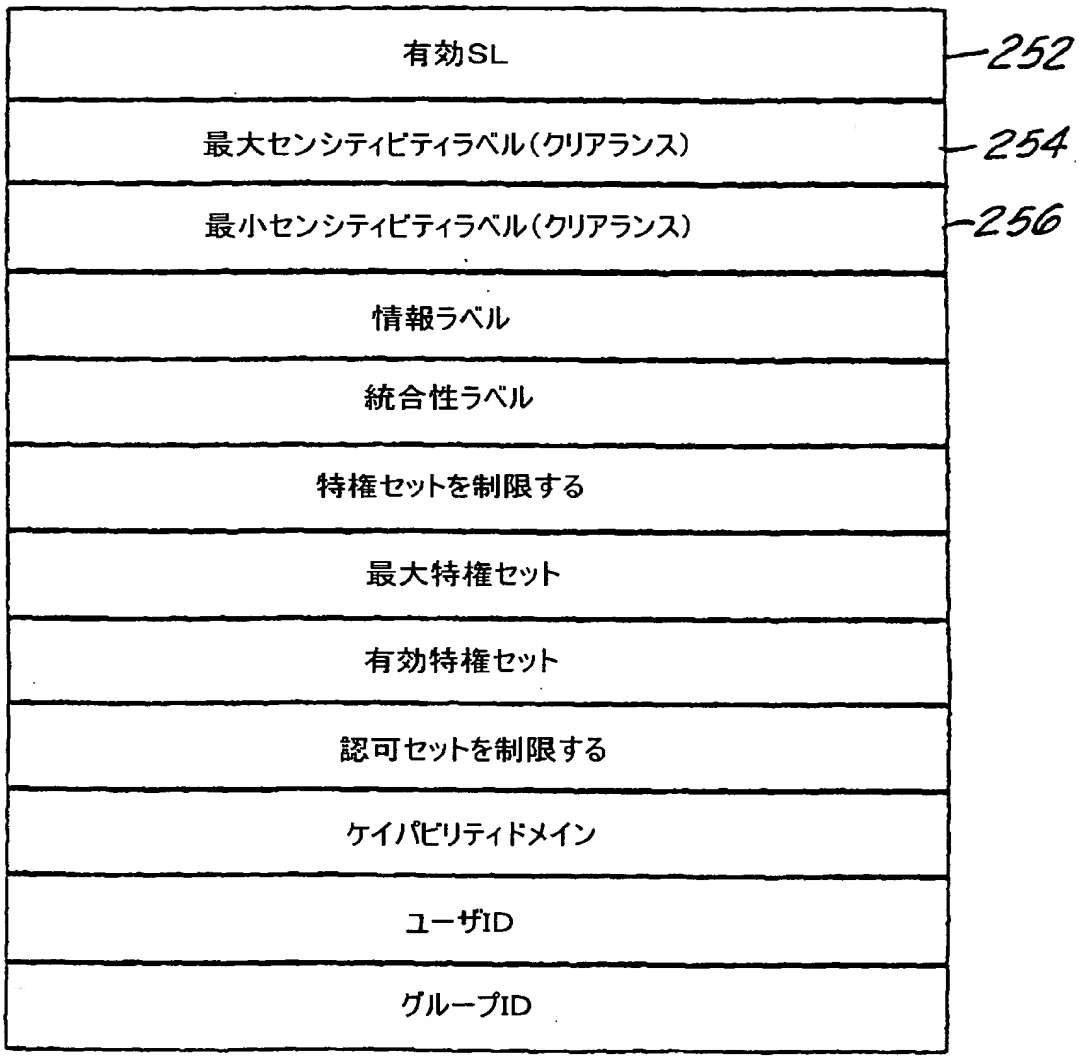

1
2
VPN
https
3
SSLプロキシ
3
SSLプロキシ
https
2
VPN
1
http
アップグレード/
ダウングレード
エンフォーサ
http
4
エスクトラネットA
5
エスクトラネットB
ADMIN
6
デフォルト
7
8
セキュリティ
ゲート
セキュリティ
ゲート
9
認証
モジュール
10
アプリケーション
1
インターネット
ウルトラスパークサーバ
LAN
レガシーアプリケーション
サーバ 1
レガシー
アプリケーション
サーバ 2

【図２】


200
Iノード内に記憶された情報
センシティビティラベル
202
最大センシティビティラベル
206
最小センシティビティラベル
情報ラベル
統合性ラベル
固有の特権
認可された特権
216
ファイルセキュリティフラグ（TCBフラグを含む）
218
ケイパビリティドメイン
アクセス認可セット
219
特権認可セット
220
ユーザID
グループID

【図３】

プロセス/パケットのセキュリティ属性



【図4】

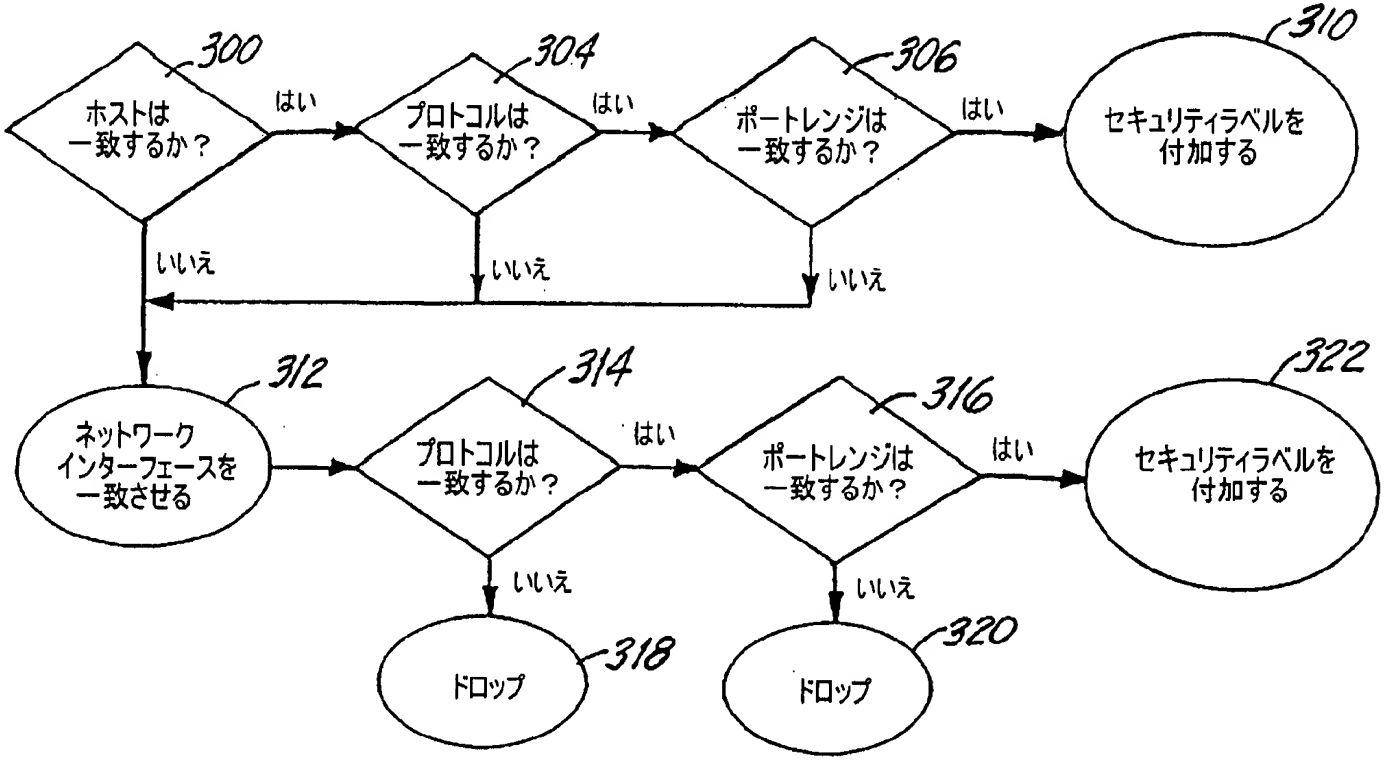
属性 (200)	プロセス/パケット (250)	ファイル (201)	サンプルデータプロセス (272)	サンプルデータファイル (292)
有効SL	X	X	シークレット	シークレット
最大SL(クリアランス)	X	X	トップシークレット	トップシークレット
最小SL(クリアランス)	X		コンフィデンシャル	
情報ラベル	X	X	シークレット「内部使用」	シークレット「企業ワイド」
統合性ラベル	X	X	シークレット	シークレット
特権の制限	X		PV_ASN, PV_SU, PV_MAC	
最大特権	X		PV_ASN, PV_SU	
有効特権	X		PV_ASN	
認可された特権		X		PV_PV_FILE (284)
固有の特権		X		PV_SR, PV_SU (286)
プロキシ特権		X		PV_ASN, PV_PV_PROC
認可されたセットを制限する	(インプライド)	X		CHIL, CHSL
特権認可セット		X		AUDITSYS, BOOT (282)
アクセス認可セット		X		DEBUG, MAKEIDB (280)
ケイパビリティドメイン	X	X	(in design)	(in design)
ファイルセキュリティフラグ		X		FSF_EPS, FSF_AUDIT
ユーザID	X	X	4321	22334
グループID	X	X	10	65432

【図５】

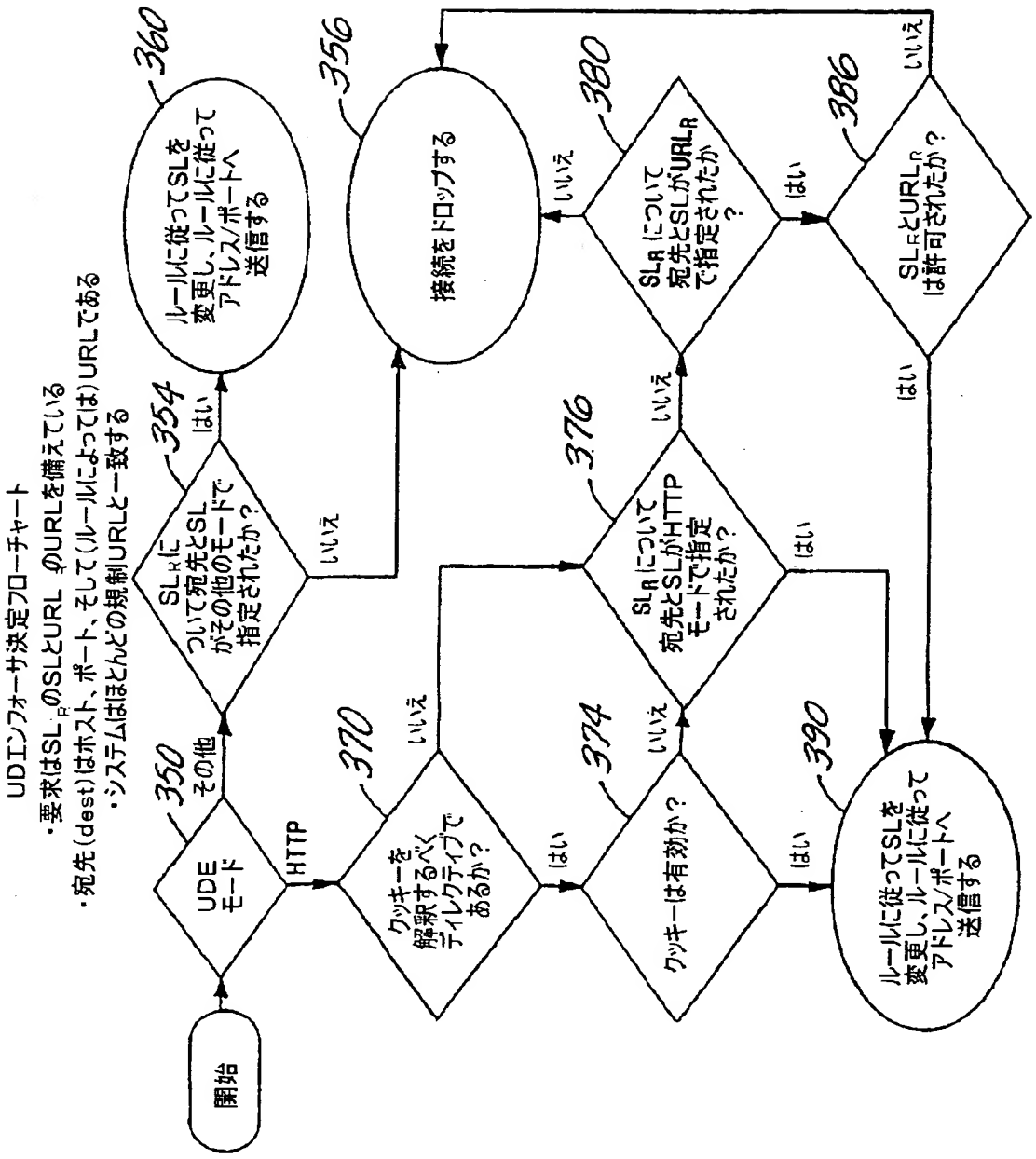
入力されるパケットの処理

入力されるパケットは以下を備えている
・ターゲットホストのアドレス
・(オプションで)指定されたプロトコル
・特定の宛先ポートまたはポートレンジ

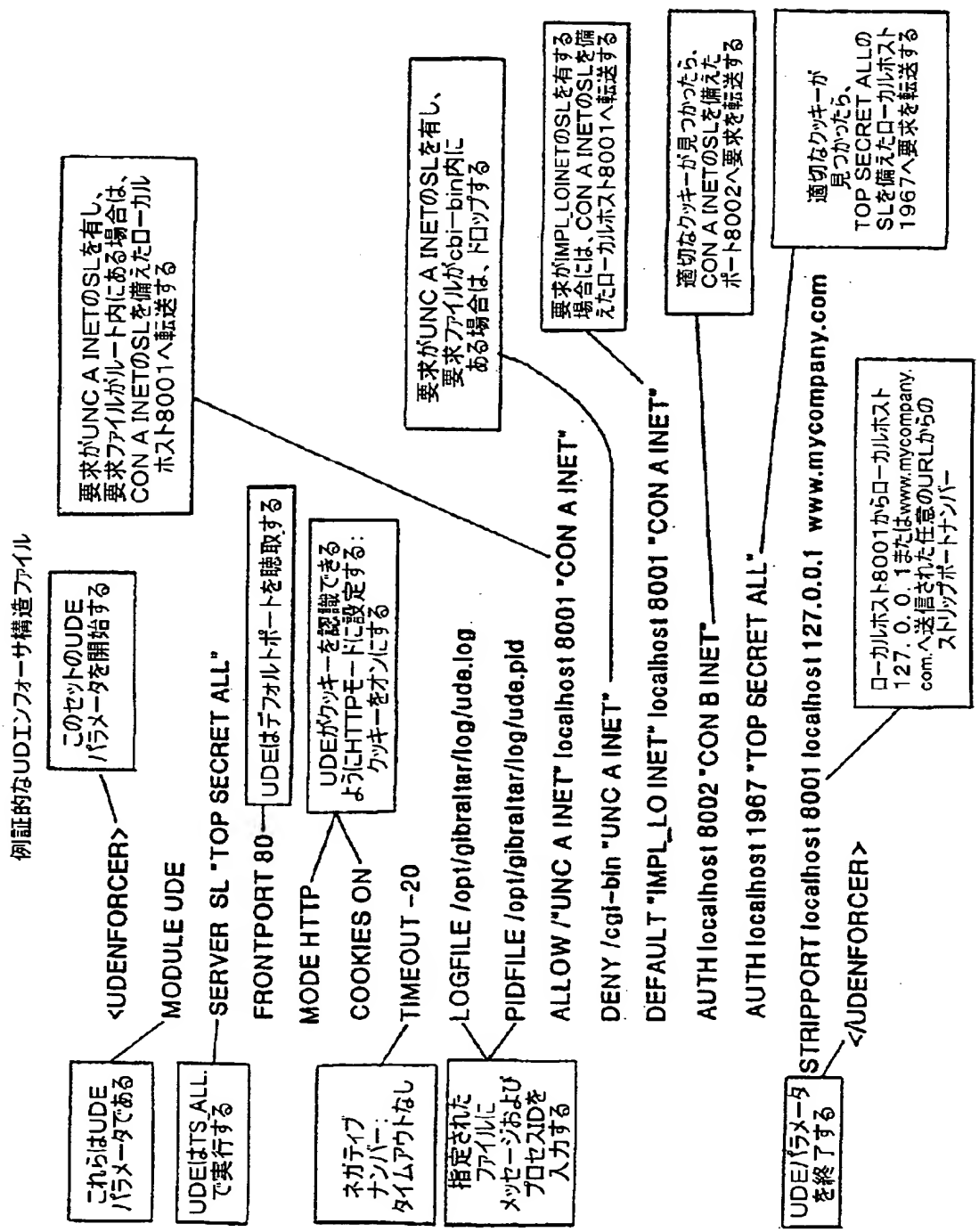
ルールのデータベースに反してこれと一致するシステム



【図６】


UDエンフォーサ決定フローチャート
・要求はSL_RのSLとURL のURLを備えている
・宛先(dest)はホスト、ポート、そして(ルールによっては)URLである
・システムはほとんどの規制URLと一致する
開始
UDE モード
350
その他
HTTP
SL_Kについて宛先とSLがその他のモードで指定されたか？
354
はい
いいえ
ルールに従ってSLを変更し、ルールに従ってアドレス/ポートへ送信する
360
接続をドロップする
356
クッキーを解釈するべくディレクティブであるか？
370
いいえ
はい
SL_Rについて宛先とSLがHTTPモードで指定されたか？
376
いいえ
はい
SL_Rについて宛先とSLがURL_Rで指定されたか？
380
いいえ
はい
SL_RとURL_Rは許可されたか？
386
いいえ
はい
クッキーは有効か？
374
いいえ
はい
ルールに従ってSLを変更し、ルールに従ってアドレス/ポートへ送信する
390

【図7】

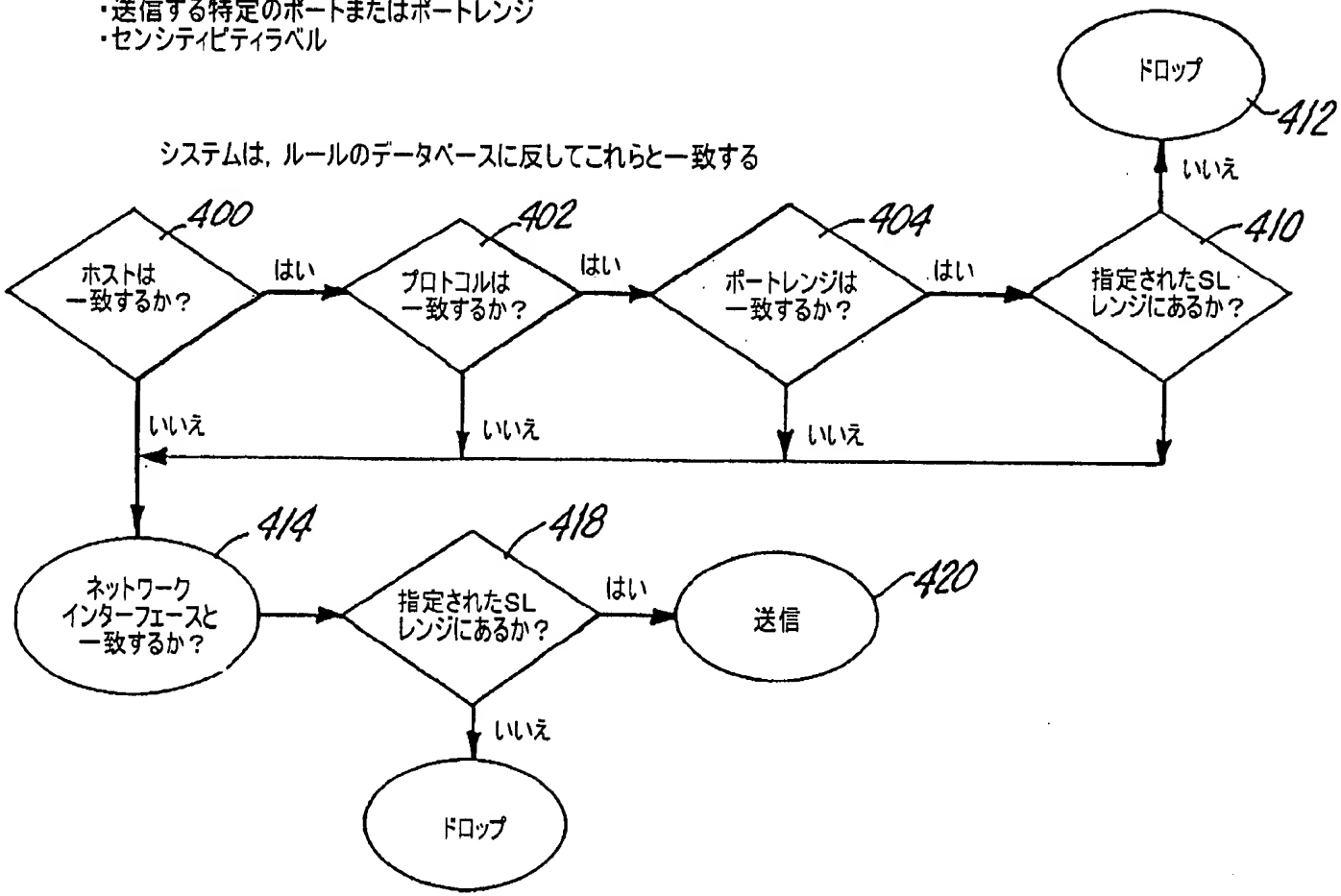

例証的なUDエンフォーサ構造ファイル
<UDENFORCER>
MODULE UDE
SERVER SL "TOP SECRET ALL"
FRONTPORT 80
MODE HTTP
COOKIES ON
TIMEOUT -20
LOGFILE /opt/gibraltar/log/ude.log
PIDFILE /opt/gibraltar/log/ude.pid
ALLOW /"UNC A INET" localhost 8001 "CON A INET"
DENY /cgi-bin "UNC A INET"
DEFAULT "IMPL_LO INET" localhost 8001 "CON A INET"
AUTH localhost 8002 "CON B INET"
AUTH localhost 1967 "TOP SECRET ALL"
STRIPPORT localhost 8001 localhost 127.0.0.1 www.mycompany.com
</UDENFORCER>
このセットのUDE パラメータを開始する
これらはUDE パラメータである
UDEはTS_ALL で実行する
UDEはデフォルトポートを聴取する
UDEがクッキーを認識できるようにHTTPモードに設定する：クッキーをオンにする
ネガティブ ナンバー；タイムアウトなし
指定されたファイルにメッセージおよびプロセスIDを入力する
要求がUNC A INETのSLを有し、要求ファイルがルート内にある場合は、CON A INETのSLを備えたローカルホスト8001へ転送する
要求がUNC A INETのSLを有し、要求ファイルがcbi-bin内にある場合は、ドロップする
要求がIMPL_LOINETのSLを有する場合には、CON A INETのSLを備えたローカルホスト8001へ転送する
適切なクッキーが見つかったら、CON A INETのSLを備えたポート8002へ要求を転送する
適切なクッキーが見つかったら、TOP SECRET ALLのSLを備えたローカルホスト1967へ要求を転送する
ローカルホスト8001からローカルホスト127.0.0.1またはwww.mycompany.com.へ送信された任意のURLからのストリップポートナンバー
UDEパラメータを終了する

【図８】

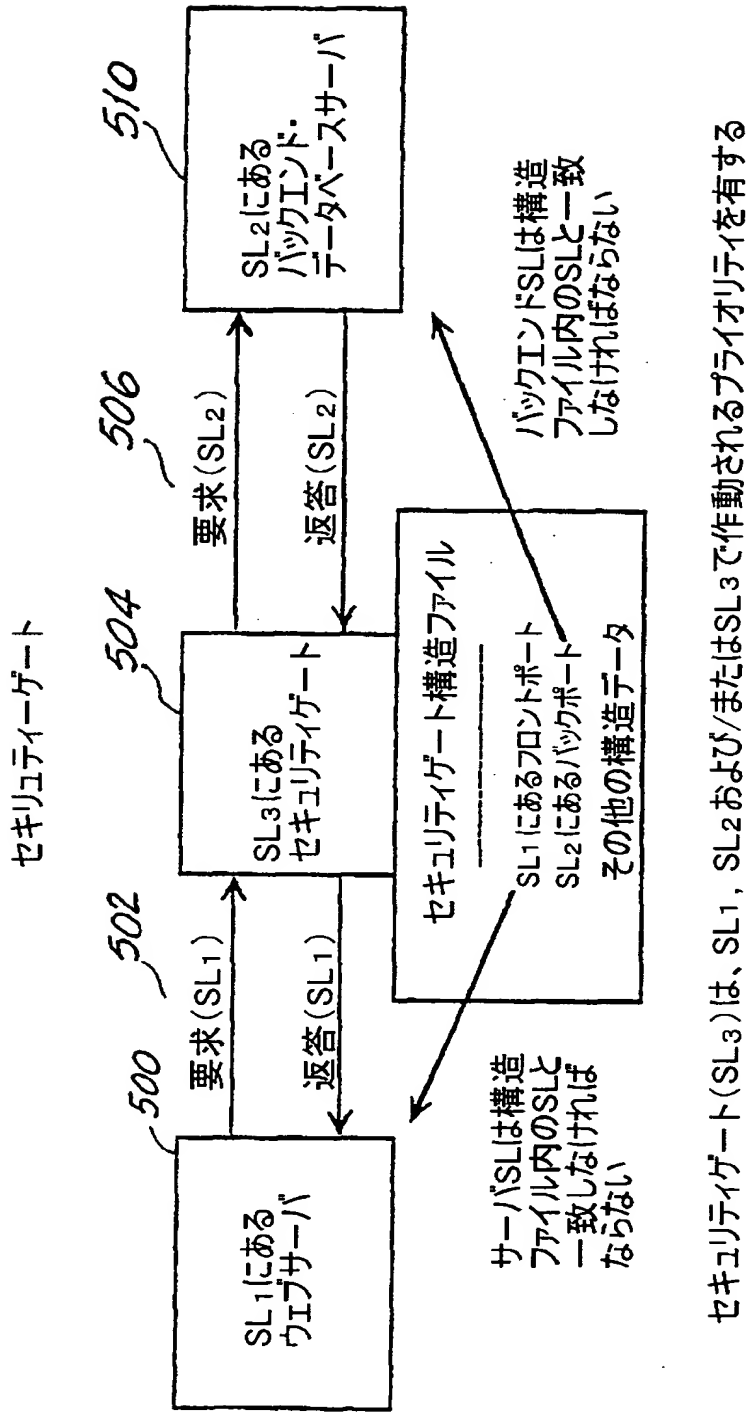
出力されるパケット処理

出力されるパケットは以下を備えている

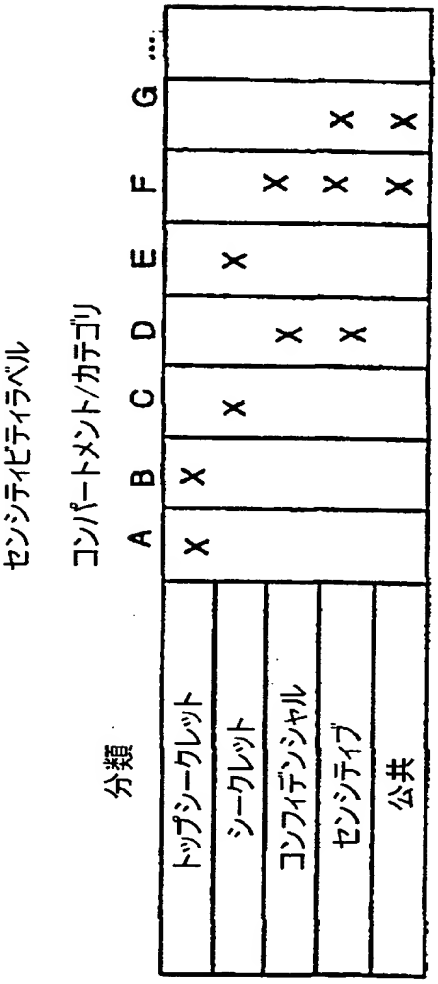
- ターゲットホストのアドレス
- (オプションで)指定されたプロトコル
- 送信する特定のポートまたはポートレンジ
- センシティビティラベル



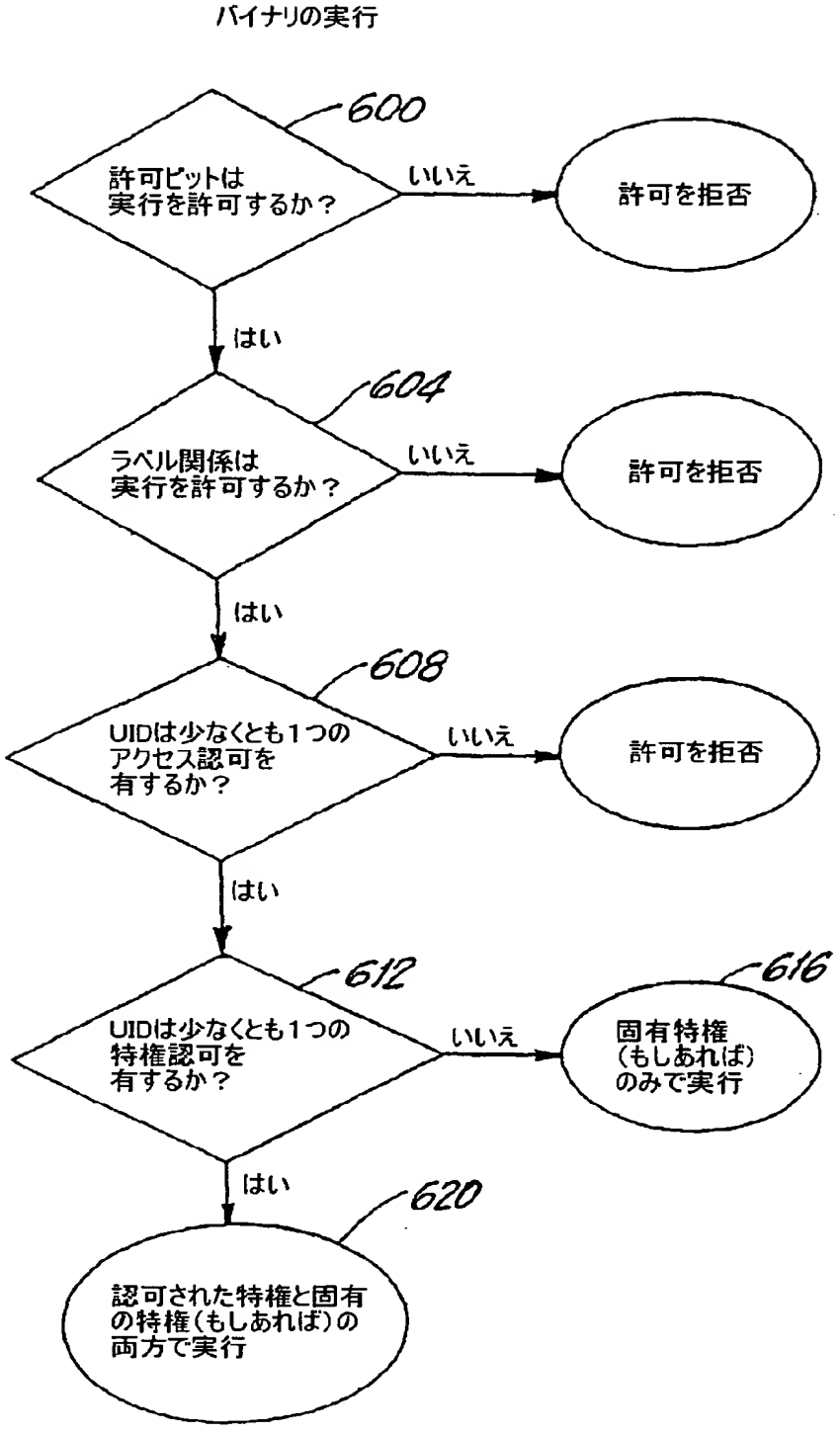
【図９】


セキュリティーゲート
500
502
504
506
510
SL1にある
ウェブサーバ
要求(SL1)
返答(SL1)
SL3にある
セキュリティゲート
要求(SL2)
返答(SL2)
SL2にある
バックエンド・
データベースサーバ
セキュリティゲート構造ファイル
SL1にあるフロントポート
SL2にあるバックポート
その他の構造データ
サーバSLは構造
ファイル内のSLと
一致しなければ
ならない
バックエンドSLは構造
ファイル内のSLと一致
しなければならない
セキュリティゲート(SL3)は、SL1，SL2およびまたはSL3で作動されるプライオリティを有する

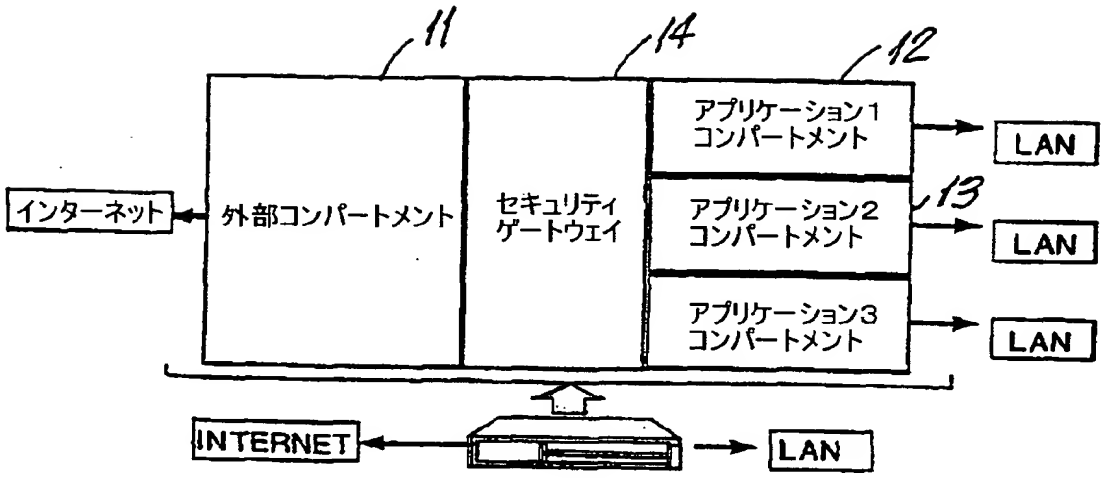
【図１０】


センシティビティラベル
コンパートメント/カテゴリ
分類
A
B
C
D
E
F
G
...
トップシークレット
シークレット
コンフィデンシャル
センシティブ
公共

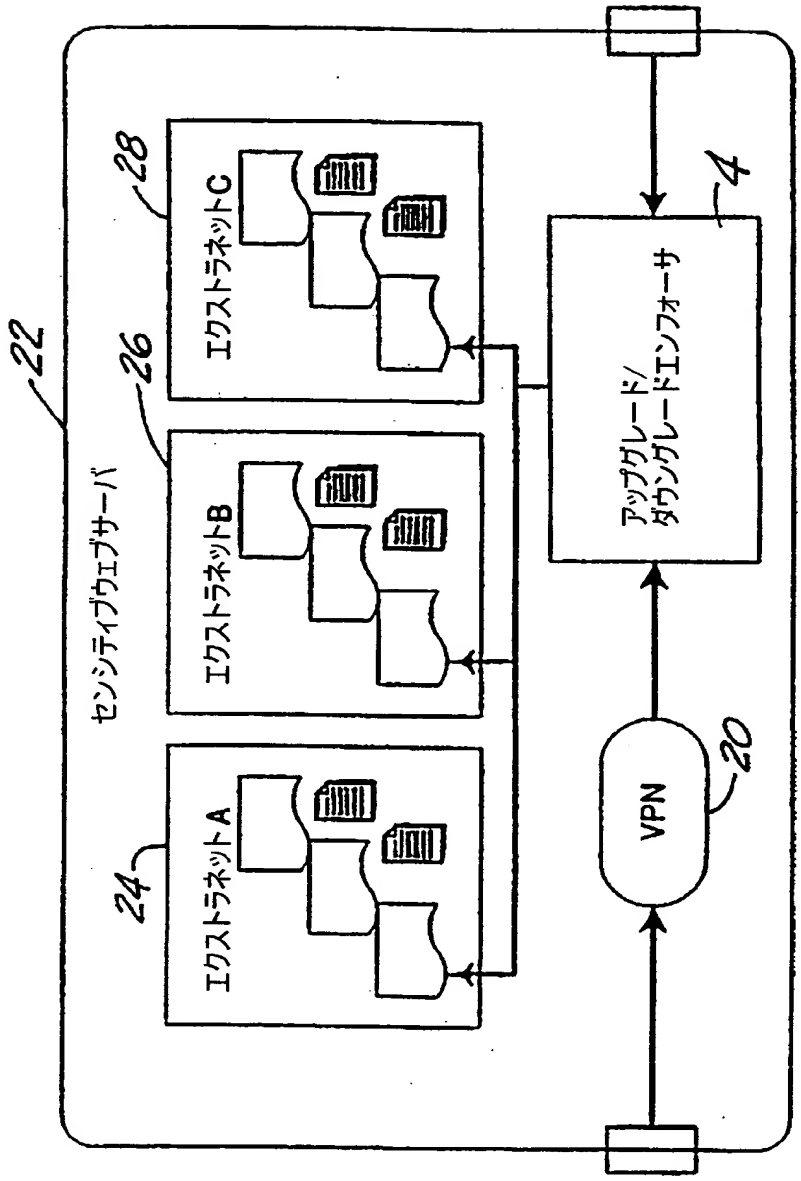
【図１１】


バイナリの実行
600
許可ビットは
実行を許可するか？
いいえ
許可を拒否
はい
604
ラベル関係は
実行を許可するか？
いいえ
許可を拒否
はい
608
UIDは少なくとも１つの
アクセス認可を
有するか？
いいえ
許可を拒否
はい
612
UIDは少なくとも１つの
特権認可を
有するか？
いいえ
616
固有特権
（もしあれば）
のみで実行
はい
620
認可された特権と固有
の特権（もしあれば）の
両方で実行

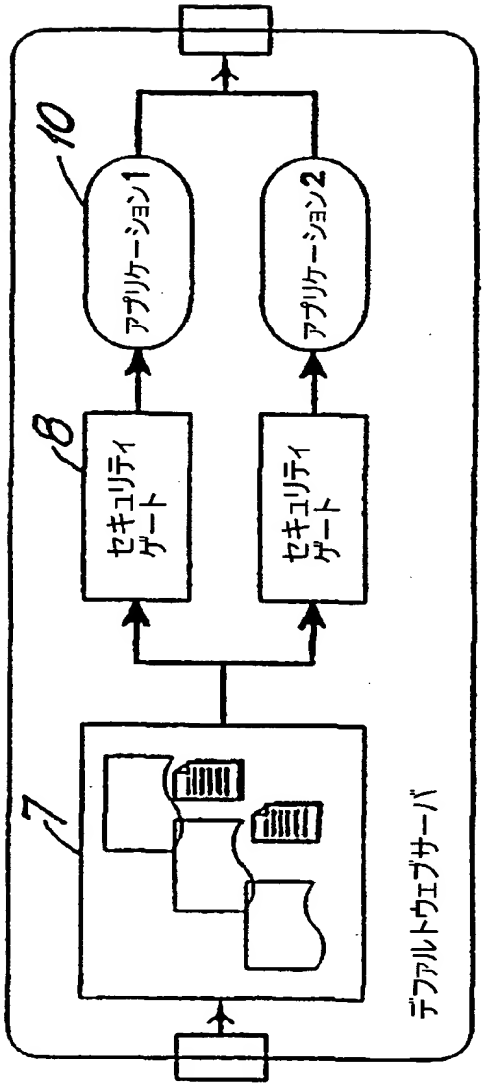
【図１２】


11
14
12
アプリケーション1
コンパートメント
LAN
インターネット
外部コンパートメント
セキュリティ
ゲートウエイ
アプリケーション2
コンパートメント
13
LAN
アプリケーション3
コンパートメント
LAN
INTERNET
LAN

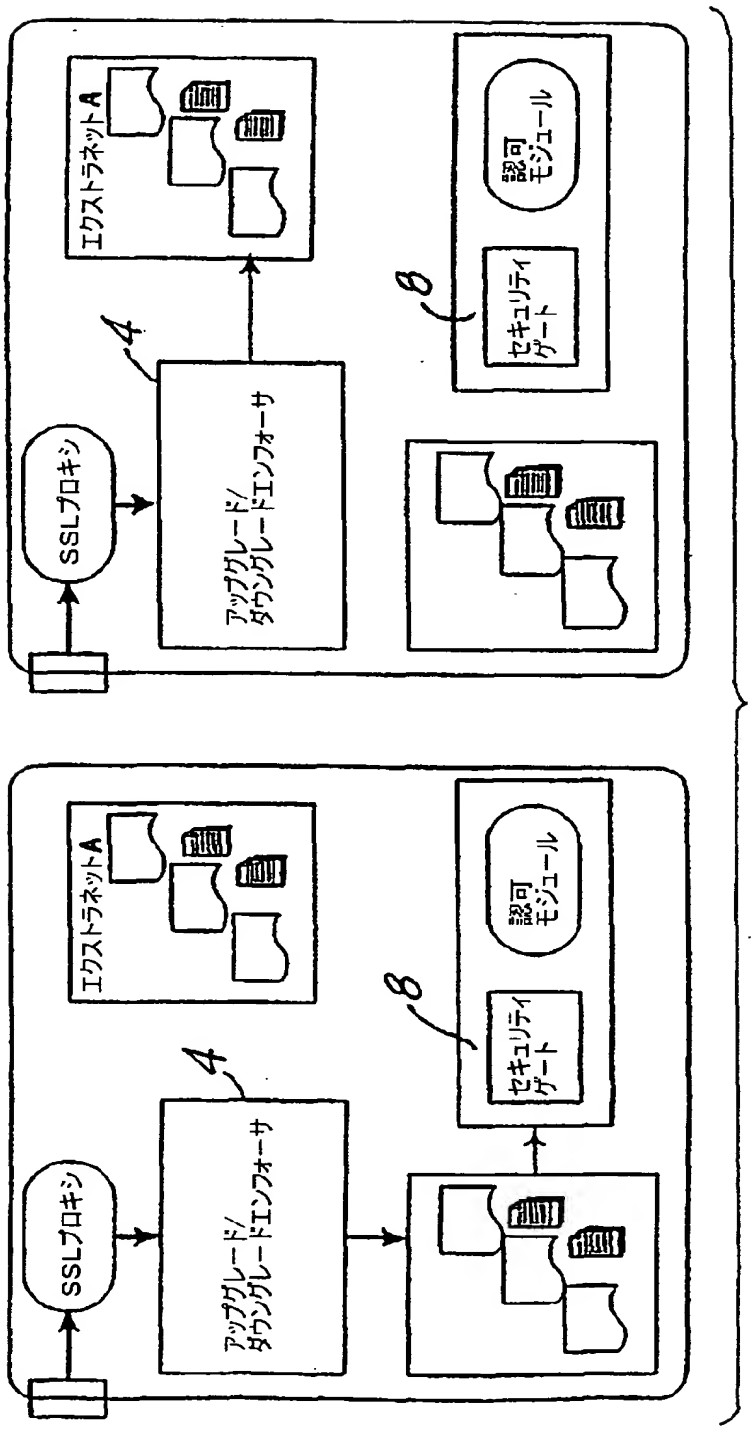
【図１３】


22
センシティブウェブサーバ
エクストラネットA
24
エクストラネットB
26
エクストラネットC
28
VPN
20
アップグレード/
ダウングレードエンフォーサ
4

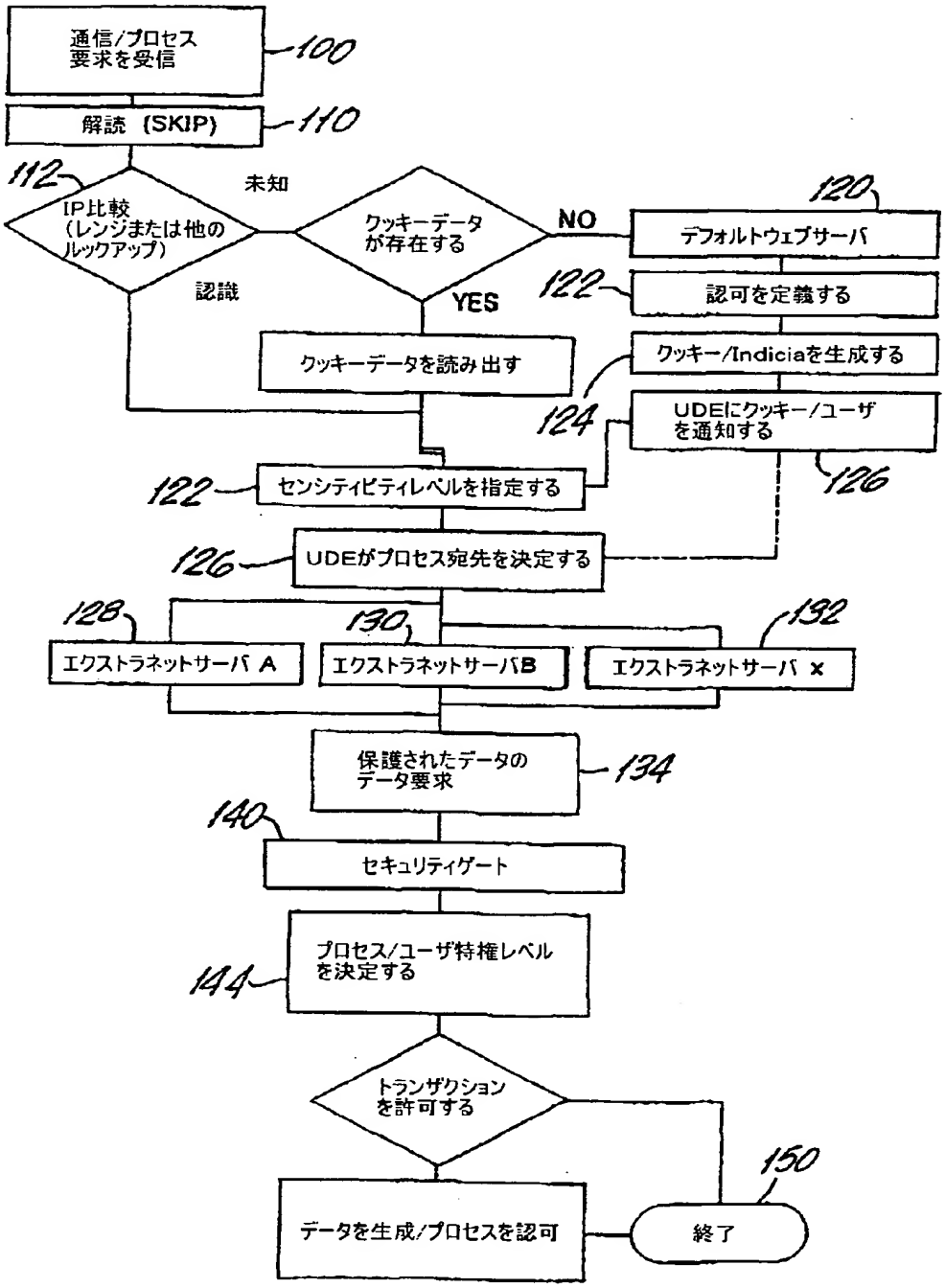
【図１４】


10
アプリケーション1
アプリケーション2
18
セキュリティゲート
セキュリティゲート
17
デファルトウェブサーバ

【図１５】


エクストラネットA
SSLプロキシ
アップグレード/
ダウングレードエンフォーサ
4
8
セキュリティ
ゲート
認可
モジュール

【図１６】


通信/プロセス
要求を受信
100
解読 (SKIP)
110
112
IP比較
(レンジまたは他の
ルックアップ)
未知
認識
クッキーデータ
が存在する
NO
YES
120
デフォルトウェブサーバ
122
認可を定義する
クッキーデータを読み出す
クッキー/Indiciaを生成する
124
UDEにクッキー/ユーザ
を通知する
126
122
センシティビティレベルを指定する
126
UDEがプロセス宛先を決定する
128
130
132
エクストラネットサーバ A
エクストラネットサーバB
エクストラネットサーバ x
保護されたデータの
データ要求
134
140
セキュリティゲート
プロセス/ユーザ特権レベル
を決定する
144
トランザクション
を許可する
150
データを生成/プロセスを認可
終了

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/22331

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :G06F 13/00
US CL :713/201
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/201, 200; 709/225, 229

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST
search terms: sensitivity levels, extended attributes

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, P	US 5,903,732 A (REED ET AL.) 11 May 1999, col. 3, line 41 - col. 8, line 4.	1-18
Y, P	US 5,845,068 A (WINIGER) 01 December 1998, col. 3, line 31 - col. 9, line 11.	1-18
X	US 5,596,718 A (BOEBERT ET AL.) 21 January 1997, col. 3, line 66 - col. 8, line 5, and col. 9, line 41 - col. 10, line 6.	19
Y	STEEN, W. et al. "NetWare Security" 31 December 1996, New Riders Publishing, Chpt 10: pp 248-277.	1-18

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 10 JANUARY 2000	Date of mailing of the international search report 07 FEB 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer STEPHEN ELMORE Joni Hill Telephone No. (703) 305-3800

Form PCT/ISA/210 (second sheet)(July 1992)*

フロントページの続き

(81)指定国　　EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW

(72)発明者　ハンソン, チャド,　ジェー.
アメリカ合衆国　61802　イリノイズ, アーバナ, イー.　ユニヴァーシティ　ナンバー8　2320

(72)発明者　サンドーン, ランドール.　ジェー.
アメリカ合衆国　61802　イリノイズ, アーバナ, カントリイ　ロード　1550　エヌ.　1779

Fターム(参考)　5B076 FA04 FB01 FD08